



Entropy accumulation with improved second-order

Frederic Dupuis, Omar Fawzi

► To cite this version:

Frederic Dupuis, Omar Fawzi. Entropy accumulation with improved second-order. 2018. hal-01925985

HAL Id: hal-01925985

<https://inria.hal.science/hal-01925985>

Preprint submitted on 18 Nov 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Entropy accumulation with improved second-order

Frédéric Dupuis¹ Omar Fawzi²

¹*Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France*

²*Université de Lyon, ENS de Lyon, CNRS, UCBL, LIP, F-69342, Lyon Cedex 07, France*

November 18, 2018

Abstract

The entropy accumulation theorem [11] states that the smooth min-entropy of an n -partite system $A = (A_1, \dots, A_n)$ is lower-bounded by the sum of the von Neumann entropies of suitably chosen conditional states up to corrections that are sublinear in n . This theorem is particularly suited to proving the security of quantum cryptographic protocols, and in particular so-called device-independent protocols for randomness expansion and key distribution, where the devices can be built and preprogrammed by a malicious supplier [2]. However, while the bounds provided by this theorem are optimal in the first order, the second-order term is bounded more crudely, in such a way that the bounds deteriorate significantly when the theorem is applied directly to protocols where parameter estimation is done by sampling a small fraction of the positions, as is done in most QKD protocols. The objective of this paper is to improve this second-order sublinear term and remedy this problem. On the way, we prove various bounds on the divergence variance, which might be of independent interest.

1 Introduction

There are many protocols in quantum cryptography, such as quantum key distribution, that work by generating randomness. Such protocols usually proceed as follows: we perform a basic subprotocol n times (for example, sending a photon in a random polarization from Alice to Bob), we then gather statistics about the protocol run (for example, we compute the error rate from a randomly chosen sample of the rounds), and we then conclude that the final state contains a certain amount of randomness, which can then be processed further. Mathematical tools that can quantify the amount of randomness produced by quantum processes therefore constitute the centerpiece of many security proofs in quantum cryptography. The entropy accumulation theorem [11] provides such a powerful tool that applies to a very general class of protocols, including device-independent protocols.

Informally, the main result of [11] is the following. Suppose we have an n -step quantum process like the one depicted in Figure 1, in which we start with

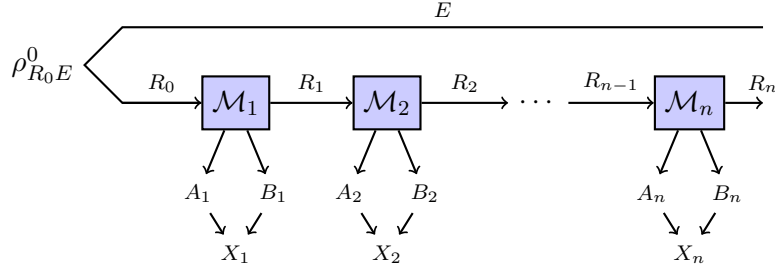


Figure 1: Illustration of the type of process that the entropy accumulation theorem applies to.

a bipartite state $\rho_{R_0 E}$ and the R_0 share of the state undergoes an n step process specified by the quantum channels \mathcal{M}_1 to \mathcal{M}_n . At step i of the process, two quantum systems A_i and B_i are produced, from which one can extract a *classical* random variable X_i . The goal is then to bound the amount of randomness present in A_1^n given B_1^n , conditioned on the string X_1^n being in a certain set Ω . The X_i 's are meant to represent the data we do statistics on, for example X_i might tell us that there is an error at position i , and we want to condition on the observed error rate being below some threshold. Stated informally, the statement proven in [11] is then

$$H_{\min}^{\epsilon}(A_1^n | B_1^n E, X_1^n \in \Omega)_{\rho} \geq n \left(\inf_{q \in \Omega} f(q) \right) - \sqrt{n}c \quad (1)$$

Here, the smooth min-entropy H_{\min}^{ϵ} represents the amount of extractable randomness (see Definition 2.7), and the *tradeoff function* $f(q)$ quantifies the worst-case amount of entropy produced by one step of the process for an input state that is consistent with observing the statistics q . One would then apply this theorem by replacing the \mathcal{M}_i 's by one step of the cryptographic protocol to obtain the desired bound. This is done, for example, in [2, 1] for device-independent randomness expansion and quantum key distribution.

While this method yields optimal bounds in the first order, the second-order term which scales as \sqrt{n} is bounded more crudely, and for some applications, this term can become dominant very quickly. This is particularly the case in applications which estimate the amount of entropy produced by testing a small fraction of the positions, which includes a large number of protocols of interest. The reason for this is that the value of c in Equation (1) is proportional to the gradient of f . Now, suppose that we have a protocol where we are testing positions with probability $O(1/n)$; in general this will make the gradient of f proportional to n and therefore the second-order term will become $\Omega(n^{3/2})$ and overwhelm the first-order term. This is worse than we would expect: when we perform the analysis using conventional tools such as Chernoff-Hoeffding bounds in cases that are amenable to it, we obtain a much better scaling behavior, and in particular we still expect a non-trivial bound when the testing rate is $O(1/n)$. As a further indication that the second-order term can be improved, we also

note that in [2, Appendix B], they resort to applying the entropy accumulation theorem to blocks rather than single rounds in order to obtain a good dependence on the testing rate.

The goal of this paper is therefore to improve the second-order term in (1). Analyzing second-order correction terms is already commonplace in information theory ever since the 60s, with the work of Volker Strassen [23] who gave second-order bounds for hypothesis testing and channel coding. This topic has also seen a revival more recently [12, 22, 21]. Quantum versions of such bounds have been proven as well since then; for example, Li [14] and Tomamichel and Hayashi [28] have shown a second-order expansion for quantum hypothesis testing, and [28] additionally gives second-order expansions for several other entropic quantities of interest. Other more recent developments can also be found in [30, 29, 13, 4, 3, 8, 9].

Most of these results go one step further than we will in this paper, in that they pin down the $O(\sqrt{n})$ term *exactly*, usually by employing some form of the Berry-Esseen theorem to a carefully designed classical random variable. Unfortunately, this approach seems to fail here, and we must resort to slightly weaker bounds that nevertheless give the right scaling behavior for protocols with infrequent sampling, and that are largely good enough in practice.

Paper organization: In Section 2, we give the notation used and some preliminary facts needed for the rest of the paper, including the Rényi entropy chain rule that powers the original entropy accumulation result in Section 2.3. Section 3 then introduces the *divergence variance* which governs the form of the second-order term, and discusses some of its properties. In Section 4, we present a new bound for the Rényi entropy in terms of the von Neumann entropy, and then apply it to the entropy accumulation theorem in Section 5, with specific bounds for the case of protocols with infrequent sampling in Section 5.1. We then compute finite-block-size bounds for the particular application of device-independent randomness expansion in Section 6 and conclude with some open problems in Section 7.

2 Preliminaries

2.1 Notation

In the table below, we summarize some of the notation used throughout the paper:

<i>Symbol</i>	<i>Definition</i>
A, B, C, \dots	Quantum systems, and their associated Hilbert spaces
$\mathcal{L}(A, B)$	Set of linear operators from A to B
$\mathcal{L}(A)$	$\mathcal{L}(A, A)$
X_{AB}	Operator in $\mathcal{L}(A \otimes B)$
$X_{B \leftarrow A}$	Operator in $\mathcal{L}(A, B)$
$\mathcal{D}(A)$	Set of normalized density operators on A
$\mathcal{D}_{\leq}(A)$	Set of subnormalized density operators on A
$\text{Pos}(A)$	Set of positive semidefinite operators on A
$X_A \geq Y_A$	$X_A - Y_A \in \text{Pos}(A)$
A_i^j (with $j \geq i$)	Given n systems A_1, \dots, A_n , this is a shorthand for A_i, \dots, A_j
A^n	Often used as shorthand for A_1, \dots, A_n
$\log(x)$	Logarithm of x in base 2
$\text{Var}(X)$	Variance of the random variable X
$\text{Cov}(X, Y)$	Covariance of the random variables X and Y
$D_{\alpha}(\rho \parallel \sigma)$	Sandwiched Rényi divergence (Definition 2.3)
$D'_{\alpha}(\rho \parallel \sigma)$	Petz Rényi divergence (Definition 2.4)
$H_{\alpha}(A B)_{\rho}$	$-D_{\alpha}(\rho_{AB} \parallel \text{id}_A \otimes \rho_B)$
$H_{\alpha}^{\uparrow}(A B)_{\rho}$	$-\inf_{\sigma_B} D_{\alpha}(\rho_{AB} \parallel \text{id}_A \otimes \sigma_B)$
$H'_{\alpha}(A B)_{\rho}$	$-D'_{\alpha}(\rho_{AB} \parallel \text{id}_A \otimes \rho_B)$
$D_{\min}(\rho \parallel \sigma)$	$D_{\frac{1}{2}}(\rho \parallel \sigma)$
$D_{\max}(\rho \parallel \sigma)$	$D_{\infty}(\rho \parallel \sigma)$
$V(\cdot)$	Various divergence variance measures; see Section 3

2.2 Entropic quantities

The central mathematical tools used in this paper are entropic quantities, i.e. various ways of quantifying the amount of uncertainty present in classical or quantum systems. In this section, we give definitions for the quantities that will play a role in our results.

Definition 2.1 (Relative entropy). For any positive semidefinite operators ρ and σ , the *relative entropy* is defined as

$$D(\rho \parallel \sigma) = \begin{cases} \text{tr}[\rho(\log \rho - \log \sigma)] & \text{if } \text{supp}(\rho) \subseteq \text{supp}(\sigma) \\ \infty & \text{otherwise} \end{cases}.$$

Definition 2.2 (von Neumann entropy). Let $\rho_{AB} \in \mathcal{D}(AB)$ be a bipartite density operator. Then, the *conditional von Neumann entropy* is defined as

$$H(A|B)_{\rho} = -D(\rho_{AB} \parallel \text{id}_A \otimes \rho_B).$$

Our proofs heavily rely on two versions of the Rényi relative entropy: the one first introduced by Petz [18], and the “sandwiched” version introduced in [32, 16]. We define both of these here:

Definition 2.3 (Sandwiched Rényi divergence). Let ρ be a subnormalized quantum state, let σ be positive semidefinite, and let $\alpha \in [\frac{1}{2}, \infty]$. Then, the sandwiched Rényi divergence is defined as

$$D_\alpha(\rho\|\sigma) = \begin{cases} \frac{1}{\alpha-1} \log \operatorname{tr} \left[\left(\sigma^{-\frac{\alpha'}{2}} \rho \sigma^{-\frac{\alpha'}{2}} \right)^\alpha \right] & \text{if } \alpha < 1 \text{ or } \operatorname{supp}(\rho) \subseteq \operatorname{supp}(\sigma) \\ \log \inf \{ \lambda : \rho \leq \lambda \sigma \} & \text{if } \alpha = \infty \\ D(\rho\|\sigma) & \text{if } \alpha = 1 \\ \infty & \text{otherwise,} \end{cases} \quad (2)$$

where $\alpha' := \frac{\alpha-1}{\alpha}$. Note D_∞ is also referred to as D_{\max} and $D_{\frac{1}{2}}$ as D_{\min} .

Definition 2.4 (Petz Rényi divergence). Let ρ be a subnormalized quantum state, let σ be positive semidefinite, and let $\alpha \in [0, 2]$. Then, the Petz Rényi divergence is defined as

$$D'_\alpha(\rho\|\sigma) = \begin{cases} \frac{1}{\alpha-1} \log \operatorname{tr} [\rho^\alpha \sigma^{1-\alpha}] & \text{if } 0 < \alpha < 1 \text{ or } \operatorname{supp}(\rho) \subseteq \operatorname{supp}(\sigma) \\ -\log \operatorname{tr} [\Pi_{\operatorname{supp}(\rho)} \sigma] & \text{if } \alpha = 0 \\ D(\rho\|\sigma) & \text{if } \alpha = 1 \\ \infty & \text{otherwise,} \end{cases} \quad (3)$$

where $\Pi_{\operatorname{supp}(\rho)}$ is the projector on the support of ρ .

These relative entropies can be used to define a conditional entropy:

Definition 2.5 (Sandwiched Rényi conditional entropy). For any density operator ρ_{AB} and for $\alpha \in [\frac{1}{2}, \infty)$ the *sandwiched α -Rényi entropy of A conditioned on B* is defined as

$$H_\alpha(A|B)_\rho = -D_\alpha(\rho_{AB}\|\operatorname{id}_A \otimes \rho_B).$$

Note that we also refer to $H_\infty(A|B)_\rho$ as $H_{\min}(A|B)_{\rho|B}$.

It turns out that there are multiple ways of defining conditional entropies from relative entropies. Another variant that will be needed in this work is the following:

Definition 2.6. For any density operator ρ_{AB} and for $\alpha \in (0, 1) \cup (1, \infty)$, we define

$$H_\alpha^\uparrow(A|B)_\rho = -\inf_{\sigma_B} D_\alpha(\rho_{AB}\|\operatorname{id}_A \otimes \sigma_B)$$

where the infimum is over all subnormalized density operators on B . Note that we also refer to $H_\infty^\uparrow(A|B)_\rho$ as $H_{\min}^\uparrow(A|B)_\rho$, called the *min-entropy*, and to $H_{\frac{1}{2}}^\uparrow(A|B)_\rho$ as $H_{\max}(A|B)_\rho$, called the *max-entropy*.

Finally, in the case of the min-entropy, we will also need the following smooth versions:

Definition 2.7. For any density operator ρ_{AB} and for $\varepsilon \in [0, 1]$ the ε -smooth min- and max-entropies of A conditioned on B are

$$H_{\min}^{\varepsilon}(A|B)_{\rho} = \sup_{\tilde{\rho}} H_{\min}(A|B)_{\tilde{\rho}}$$

$$H_{\max}^{\varepsilon}(A|B)_{\rho} = \inf_{\tilde{\rho}} H_{\max}(A|B)_{\tilde{\rho}},$$

respectively, where $\tilde{\rho}$ is any subnormalized density operator that is ε -close to ρ in terms of the purified distance [27, 24].

2.3 Chain rule for Rényi entropies

In [11], the central piece of the proof was a chain rule for Rényi entropies. As our proof largely follows the same steps, we reproduce the most relevant statement here for the reader's convenience. For the proofs, we refer the reader to [11].

Corollary 2.8 (Corollary 3.4 in [11]). *Let $\rho_{RA_1B_1}^0$ be a density operator on $R \otimes A_1 \otimes B_1$ and $\mathcal{M} = \mathcal{M}_{A_2B_2 \leftarrow R}$ be a TPCP map. Assuming that $\rho_{A_1B_1A_2B_2} = \mathcal{M}(\rho_{RA_1B_1}^0)$ satisfies the Markov condition $A_1 \leftrightarrow B_1 \leftrightarrow B_2$, we have for $\alpha \in [\frac{1}{2}, \infty)$*

$$\inf_{\omega} H_{\alpha}(A_2|B_2A_1B_1)_{\mathcal{M}(\omega)} \leq H_{\alpha}(A_1A_2|B_1B_2)_{\mathcal{M}(\rho^0)} - H_{\alpha}(A_1|B_1)_{\rho^0} \leq \sup_{\omega} H_{\alpha}(A_2|B_2A_1B_1)_{\mathcal{M}(\omega)}$$

where the supremum and infimum range over density operators $\omega_{RA_1B_1}$ on $R \otimes A_1 \otimes B_1$. Moreover, if $\rho_{RA_1B_1}^0$ is pure then we can optimise over pure states $\omega_{RA_1B_1}$.

3 The quantum divergence variance and its properties

The second-order term in our main result will be governed by a quantity called the quantum divergence variance, defined as follows:

Definition 3.1 (Quantum divergence variance). Let ρ, σ be positive semidefinite operators such that $D(\rho||\sigma)$ is finite (i.e. $\text{supp}(\rho) \subseteq \text{supp}(\sigma)$). Then, the quantum divergence variance $V(\rho||\sigma)$ is defined as:

$$V(\rho||\sigma) := \text{tr} [\rho(\log \rho - \log \sigma - \text{id} D(\rho||\sigma))^2]$$

$$= \text{tr} [\rho(\log \rho - \log \sigma)^2] - D(\rho||\sigma)^2.$$

This was already defined in [28, 14] under the names “quantum information variance” and “quantum relative variance” respectively; we instead choose a different name to clearly mark its relation to the divergence and to avoid confusion with the other variances that we are about to define.

Definition 3.2. Let ρ_{AB} be a bipartite quantum state. Then, the *quantum conditional entropy variance* $V(A|B)_{\rho}$ is given by:

$$V(A|B)_{\rho} := V(\rho_{AB}||\text{id}_A \otimes \rho_B).$$

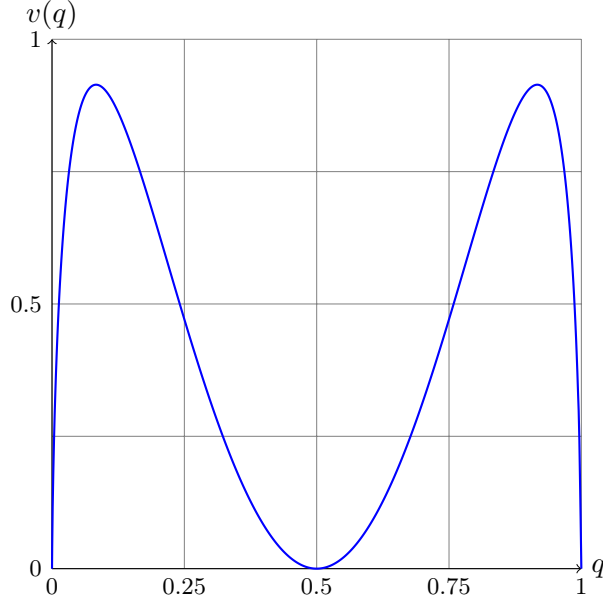


Figure 2: Plot of $v(q) = V(X)$, where X is a Bernoulli RV with $\Pr[X = 0] = q$. It peaks at around $v(0.083) \approx 0.9142$.

Of course, the system in the conditioning can be omitted in the unconditional case. Likewise, the *quantum mutual information variance* is given by:

$$V(A; B)_\rho := V(\rho_{AB} \| \rho_A \otimes \rho_B).$$

These various quantities have a number of elementary properties that we prove here. First, to get a sense of what the divergence variance looks like in a simple case, we plot the divergence variance of a single bit X with $\Pr[X = 0]$ in Figure 2. We also note that the divergence variance does not satisfy the data processing inequality, even in the classical case; in other words, it is not true in general that $V(\rho \| \sigma) \geq V(\mathcal{E}(\rho) \| \mathcal{E}(\sigma))$ for a quantum channel \mathcal{E} . To see this, consider the following counterexample: let $\rho = |0\rangle\langle 0|$, $\sigma = \text{id}$, and let \mathcal{E} be a binary symmetric channel in the computational basis with error rate 0.083. Then, we can see from the plot in Figure 2 that $V(\mathcal{E}(\rho) \| \mathcal{E}(\sigma)) > V(\rho \| \sigma)$. It is also easy to see that the opposite inequality is also false in general.

Now, we show that the divergence variance obeys the following basic bounds:

Lemma 3.3 (General bounds). *For any positive semidefinite operators ρ, σ , with $\text{supp}(\rho) \subseteq \text{supp}(\sigma)$, and any $\nu \in (0, 1)$,*

$$V(\rho \| \sigma) \leq \frac{1}{\nu^2} \log^2 \left(2^{-\nu D(\rho \| \sigma) + \nu D'_{1+\nu}(\rho \| \sigma)} + 2^{\nu D(\rho \| \sigma) - \nu D'_{1-\nu}(\rho \| \sigma)} + 1 \right). \quad (4)$$

Proof. First, without loss of generality, we restrict the space to the support of σ . We then proceed in a way similar to [25, Lemma 8]. We introduce $X =$

$2^{-D(\rho\|\sigma)}\rho \otimes (\sigma^{-1})^T, |\varphi\rangle = (\sqrt{\rho} \otimes \text{id})|\gamma\rangle$ with $|\gamma\rangle = \sum_i |i\rangle \otimes |i\rangle$. We then have $V(\rho\|\sigma) = \frac{1}{\ln^2 2} \langle \varphi | \ln^2 X | \varphi \rangle$. Observe that we have for $\nu \in (0, 1)$ and any $t > 0$

$$\begin{aligned} \ln^2 t &= \frac{1}{\nu^2} \ln^2 t^\nu \\ &\leq \frac{1}{\nu^2} \left(\ln \left(t^\nu + \frac{1}{t^\nu} \right) \right)^2 \\ &\leq \frac{1}{\nu^2} \left(\ln \left(t^\nu + \frac{1}{t^\nu} + 1 \right) \right)^2, \end{aligned}$$

where in the first inequality, we used the fact that $\ln(x)^2 \leq \ln(x + \frac{1}{x})^2$ for any $x > 0$ and in the second inequality the fact that $x + \frac{1}{x} \geq 1$. As a result, we have that

$$(\Pi_{\text{supp}(\rho)} \otimes \text{id}) \ln^2 X (\Pi_{\text{supp}(\rho)} \otimes \text{id}) \leq \frac{1}{\nu^2} (\Pi_{\text{supp}(\rho)} \otimes \text{id}) \left(\ln \left(X^\nu + \frac{\text{id}}{X^\nu} + \text{id} \right) \right)^2 (\Pi_{\text{supp}(\rho)} \otimes \text{id})$$

and therefore

$$\langle \varphi | \ln^2 X | \varphi \rangle \leq \frac{1}{\nu^2} \langle \varphi | \left(\ln \left(X^\nu + \frac{\text{id}}{X^\nu} + \text{id} \right) \right)^2 | \varphi \rangle,$$

We now use the fact that the function $s \mapsto \ln^2(s)$ is concave on the interval $[e, +\infty)$ and that $|\varphi\rangle$ is in the span of the eigenvectors of $X^\nu + \frac{\text{id}}{X^\nu} + \text{id}$ with eigenvalues in $[3, \infty)$ to get

$$\langle \varphi | \ln^2 X | \varphi \rangle \leq \frac{1}{\nu^2} \ln^2 \left(\langle \varphi | X^\nu | \varphi \rangle + \langle \varphi | \frac{\text{id}}{X^\nu} | \varphi \rangle + 1 \right).$$

But observe that

$$\langle \varphi | X^\nu | \varphi \rangle = 2^{-\nu D(\rho\|\sigma)} \text{tr}(\rho^{1+\nu} \sigma^{-\nu}) = 2^{-\nu D(\rho\|\sigma) + \nu D'_{1+\nu}(\rho\|\sigma)}$$

and

$$\langle \varphi | \frac{\text{id}}{X^\nu} | \varphi \rangle = 2^{+\nu D(\rho\|\sigma)} \text{tr}(\rho^{1-\nu} \sigma^\nu) = 2^{+\nu D(\rho\|\sigma) - \nu D'_{1-\nu}(\rho\|\sigma)}.$$

□

This leads to the following bounds for the conditional entropy variance and the mutual information variance:

Corollary 3.4. *For any density operator ρ_{AB} , we have*

$$\begin{aligned} V(A|B)_\rho &\leq \log^2(2d_A^2 + 1) \\ V(A; B)_\rho &\leq 4 \log^2(2d_A + 1). \end{aligned}$$

Proof. For the upper bound on $V(A|B)_\rho = V(\rho_{AB} \|\text{id}_A \otimes \rho_B)$ we use (4) with ν approaching 1:

$$\begin{aligned} V(A|B)_\rho &\leq \frac{1}{\nu^2} \log^2 \left(2^{-\nu D(\rho_{AB} \|\text{id}_A \otimes \rho_B) + \nu D'_{1+\nu}(\rho_{AB} \|\text{id}_A \otimes \rho_B)} + 2^{\nu D(\rho_{AB} \|\text{id}_A \otimes \rho_B) - \nu D'_{1-\nu}(\rho_{AB} \|\text{id}_A \otimes \rho_B)} + 1 \right) \\ &= \frac{1}{\nu^2} \log^2 \left(2^{\nu(H(A|B)_\rho - H'_{1+\nu}(A|B)_\rho)} + 2^{\nu(-H(A|B)_\rho + H'_{1-\nu}(A|B)_\rho)} + 1 \right) \\ &\leq \frac{1}{\nu^2} \log^2(2d_A^2 + 1). \end{aligned}$$

Taking the limit $\nu \rightarrow 1$, we get the desired result.

For the bound on $V(A; B) = V(\rho_{AB} \| \rho_A \otimes \rho_B)$, we use (4) with $\nu = \frac{1}{2}$ to have an upper bound of the form

$$\begin{aligned} V(A; B)_\rho &\leq 4 \log^2 \left(2^{-\frac{1}{2}D(\rho_{AB} \| \rho_A \otimes \rho_B) + \frac{1}{2}D'_{\frac{3}{2}}(\rho_{AB} \| \rho_A \otimes \rho_B)} + 2^{\frac{1}{2}D(\rho_{AB} \| \rho_A \otimes \rho_B) - \frac{1}{2}D'_{\frac{1}{2}}(\rho_{AB} \| \rho_A \otimes \rho_B)} + 1 \right) \\ &\leq 4 \log^2 \left(2^{\frac{1}{2}D_{\frac{3}{2}}(\rho_{AB} \| \rho_A \otimes \rho_B)} + d_A + 1 \right). \end{aligned}$$

To conclude, it suffices to show that $D_{\frac{3}{2}}(\rho_{AB} \| \rho_A \otimes \rho_B) \leq 2 \log d_A$. To do this, let ρ_{ABC} be a purification of ρ . We then have that:

$$\begin{aligned} D_{\frac{3}{2}}(\rho_{AB} \| \rho_A \otimes \rho_B) &\leq D_{\frac{3}{2}}(\rho_{ABC} \| \rho_A \otimes \rho_{BC}) \\ &= 2 \log \operatorname{tr} \left[\rho_{ABC}^{\frac{3}{2}} (\rho_A \otimes \rho_{BC})^{-\frac{1}{2}} \right] \\ &\leq 2 \log \sqrt{\operatorname{tr} \left[\rho_{ABC}^{\frac{3}{2}} \rho_A^{-1} \right] \operatorname{tr} \left[\rho_{ABC}^{\frac{3}{2}} \rho_{BC}^{-1} \right]} \\ &= \log [\operatorname{tr} [\rho_{ABC} \rho_A^{-1}] \operatorname{tr} [\rho_{ABC} \rho_{BC}^{-1}]] \\ &\leq \log d_A + \log \dim \operatorname{supp}(\rho_{BC}) \\ &\leq 2 \log d_A. \end{aligned}$$

□

Next, we show that the divergence variance is additive, in the following sense:

Lemma 3.5 (Additivity of the divergence variance). *Let ρ, τ be density operators and σ, ω be positive semidefinite operators. Then,*

$$V(\rho \otimes \tau \| \sigma \otimes \omega) = V(\rho \| \sigma) + V(\tau \| \omega).$$

Proof. We have that

$$\begin{aligned} &V(\rho \otimes \tau \| \sigma \otimes \omega) \\ &= \operatorname{tr} \left[(\rho \otimes \tau) (\log(\rho \otimes \tau) - \log(\sigma \otimes \omega) - \operatorname{id} D(\rho \| \sigma) - \operatorname{id} D(\tau \| \omega))^2 \right] \\ &= \operatorname{tr} \left[(\rho \otimes \tau) (\log \rho \otimes \operatorname{id} + \operatorname{id} \otimes \log \tau - \log \sigma \otimes \operatorname{id} - \operatorname{id} \otimes \log \omega - \operatorname{id} D(\rho \| \sigma) - \operatorname{id} D(\tau \| \omega))^2 \right] \\ &= \operatorname{tr} \left[(\rho \otimes \tau) (\log \rho \otimes \operatorname{id} - \log \sigma \otimes \operatorname{id} - \operatorname{id} D(\rho \| \sigma))^2 \right] \\ &\quad + \operatorname{tr} \left[(\rho \otimes \tau) (\operatorname{id} \otimes \log \tau - \operatorname{id} \otimes \log \omega - \operatorname{id} D(\tau \| \omega))^2 \right] \\ &\quad + \operatorname{tr} [(\rho \otimes \tau) (\log \rho \otimes \operatorname{id} - \log \sigma \otimes \operatorname{id} - \operatorname{id} D(\rho \| \sigma)) (\operatorname{id} \otimes \log \tau - \operatorname{id} \otimes \log \omega - \operatorname{id} D(\tau \| \omega))] \\ &\quad + \operatorname{tr} [(\rho \otimes \tau) (\operatorname{id} \otimes \log \tau - \operatorname{id} \otimes \log \omega - \operatorname{id} D(\tau \| \omega)) (\log \rho \otimes \operatorname{id} - \log \sigma \otimes \operatorname{id} - \operatorname{id} D(\rho \| \sigma))] \\ &= V(\rho \| \sigma) + V(\tau \| \omega) \\ &\quad + 2 \operatorname{tr} [\rho (\log \rho - \log \sigma - \operatorname{id} D(\rho \| \sigma))] \operatorname{tr} [\tau (\log \tau - \log \omega - \operatorname{id} D(\tau \| \omega))] \\ &= V(\rho \| \sigma) + V(\tau \| \omega). \end{aligned}$$

□

We also show that a conditional entropy variance with a classical variable X in the conditioning admits a decomposition in terms of the possible values of X :

Lemma 3.6. *Let ρ_{ABX} be a tripartite state with X classical. Then,*

$$V(A|BX)_\rho = \sum_x p_x V(A|B, X=x) + \text{Var}(W)$$

where W is a random variable that takes value $H(A|B, X=x)$ with probability p_x . In particular,

$$V(A|BX)_\rho \geq \sum_x p_x V(A|B, X=x).$$

Proof. We have that

$$\begin{aligned} V(A|BX)_\rho &= \text{tr} \left[\rho_{ABX} (\log \rho_{ABX} - \text{id}_A \otimes \log \rho_{BX})^2 \right] - H(A|BX)^2 \\ &= \sum_x p_x \text{tr} \left[\rho_{AB|X=x} (\log \rho_{AB|X=x} + \text{id} \log p_x - \text{id}_A \otimes \log \rho_{B|X=x} - \text{id} \log p_x)^2 \right] \\ &\quad - H(A|BX)^2 \\ &= \sum_x p_x \text{tr} \left[\rho_{AB|X=x} (\log \rho_{AB|X=x} - \text{id}_A \otimes \log \rho_{B|X=x})^2 \right] \\ &\quad - \left(\sum_x p_x H(A|B, X=x) \right)^2 \\ &= \sum_x p_x (V(A|B, X=x) + H(A|B, X=x)^2) - \left(\sum_x p_x H(A|B, X=x) \right)^2 \\ &= \sum_x p_x V(A|B, X=x) - \left(\sum_x p_x H(A|B, X=x) \right)^2 + \sum_x p_x H(A|B, X=x)^2 \\ &= \sum_x p_x V(A|B, X=x) - (\mathbb{E}W)^2 + \mathbb{E}[W^2] \\ &= \sum_x p_x V(A|B, X=x) + \text{Var}(W). \end{aligned}$$

□

We will also need the following decomposition of the conditional entropy variance for Markov chains:

Lemma 3.7. *Let ρ_{ABCDX} be a quantum state with X classical satisfying the Markov chain $AC \leftrightarrow X \leftrightarrow BD$; i.e. $I(AC; BD|X) = 0$. Then,*

$$V(AB|CDX) = V(A|CX) + V(B|DX) + 2 \text{Cov}(W_1, W_2),$$

where W_1 and W_2 are random variables that take value $H(A|C, X=x)$ and $H(B|D, X=x)$ according to the value of X , respectively. In particular, this shows that for a trivial B system, $V(A|CDX) = V(A|CX)$.

Proof. We perform the computation as follows:

$$\begin{aligned}
& V(AB|CDX) \\
&= \sum_x p_x V(AB|CD, X=x) + \text{Var}(W_1 + W_2) \\
&= \sum_x p_x (V(A|C, X=x) + V(B|D, X=x)) + \text{Var}(W_1) + \text{Var}(W_2) + 2 \text{Cov}(W_1, W_2) \\
&= V(A|CX) + V(B|DX) + 2 \text{Cov}(W_1, W_2),
\end{aligned}$$

where the first equality follows from Lemma 3.6, and the second equality from Lemma 3.5. \square

Finally, the following more specialized lemmas will be needed in the proof of our main result:

Lemma 3.8. *Let $\rho_{ACD\bar{D}X}$ be a quantum state with X classical that can be written as*

$$\sum_x p_x |x\rangle\langle x|_X \otimes \rho_{AC}^{(x)} \otimes \tau_{D\bar{D}}^{(x)}$$

with $\tau_{D\bar{D}}^{(x)} = \frac{\text{id}_{D\bar{D}}}{d_{D\bar{D}}}$ for all x . Then,

$$V(ADX|C\bar{D}) \leq V(AX|C) + V(D|X\bar{D}) + 2\sqrt{V(AX|C)V(D|X\bar{D})}.$$

Proof. First, note that the chain rule together with the Markov condition gives $H(ADX|C) = H(AX|C) + H(D|X\bar{D})$. We can then proceed as follows:

$$\begin{aligned}
V(ADX|C\bar{D}) &= \sum_x p_x \text{tr} \left[\rho_{AC}^{(x)} \otimes \tau_{D\bar{D}}^{(x)} \left(\log p_x \rho_{AC}^{(x)} \otimes \text{id}_{D\bar{D}} \right. \right. \\
&\quad \left. \left. + \text{id}_{AC} \otimes \log \tau_{D\bar{D}}^{(x)} - \text{id}_{AD\bar{D}} \otimes \log \rho_C + \text{id}_{ACD\bar{D}} \log d_{D\bar{D}} + \text{id}H(ADX|C\bar{D}) \right)^2 \right] \\
&= \sum_x p_x \text{tr} \left[\rho_{AC}^{(x)} \otimes \tau_{D\bar{D}}^{(x)} \left(\log p_x \rho_{AC}^{(x)} \otimes \text{id}_{D\bar{D}} - \text{id}_{AD\bar{D}} \otimes \log \rho_C + \text{id}H(AX|C) \right)^2 \right] \\
&\quad + \sum_x p_x \text{tr} \left[\rho_{AC}^{(x)} \otimes \tau_{D\bar{D}}^{(x)} \left(\log \tau_{D\bar{D}}^{(x)} \otimes \text{id}_{AC} + \text{id}_{ACD\bar{D}} \log d_{D\bar{D}} + \text{id}H(D|X\bar{D}) \right)^2 \right] \\
&\quad + 2 \sum_x p_x \text{tr} \left[\rho_{AC}^{(x)} \otimes \tau_{D\bar{D}}^{(x)} \left(\log p_x \rho_{AC}^{(x)} \otimes \text{id}_{D\bar{D}} - \text{id}_{AD\bar{D}} \otimes \log \rho_C + \text{id}H(AX|C) \right) \right. \\
&\quad \left. \left(\log \tau_{D\bar{D}}^{(x)} \otimes \text{id}_{AC} + \text{id}_{ABD\bar{D}} \log d_{D\bar{D}} + \text{id}H(D|X\bar{D}) \right) \right] \\
&= V(AX|C) + V(D|X\bar{D}) + 2 \cdot \text{crossterm},
\end{aligned}$$

where we used in the second equality the fact that $\left(\log p_x \rho_{AC}^{(x)} \otimes \text{id}_{D\bar{D}} - \text{id}_{AD\bar{D}} \otimes \log \rho_C + \text{id}H(AX|C) \right)$ and $\left(\log \tau_{D\bar{D}}^{(x)} \otimes \text{id}_{AC} + \text{id}_{ABD\bar{D}} \log d_{D\bar{D}} + \text{id}H(D|X\bar{D}) \right)$

commute. To get the last equality, we observe that

$$\begin{aligned}
& \sum_x p_x \text{tr} \left[\rho_{AC}^{(x)} \otimes \tau_{D\bar{D}}^{(x)} \left(\log p_x \rho_{AC}^{(x)} \otimes \text{id}_{D\bar{D}} - \text{id}_{AD\bar{D}} \otimes \log \rho_C + \text{id} H(AX|C) \right)^2 \right] \\
&= \sum_x p_x \text{tr} \left[\rho_{AC}^{(x)} \left(\log p_x \rho_{AC}^{(x)} - \text{id}_A \otimes \log \rho_C + \text{id} H(AX|C) \right)^2 \right] \\
&= V(AX|C),
\end{aligned}$$

and

$$\begin{aligned}
& \sum_x p_x \text{tr} \left[\rho_{AC}^{(x)} \otimes \tau_{D\bar{D}}^{(x)} \left(\log \tau_{D\bar{D}}^{(x)} \otimes \text{id}_{AC} + \text{id}_{ACD\bar{D}} \log d_{\bar{D}} + \text{id} H(D|X\bar{D}) \right)^2 \right] \\
&= \text{tr} \left[\sum_x p_x |x\rangle\langle x| \otimes \tau_{D\bar{D}}^{(x)} \left(\log \left(\sum_x p_x |x\rangle\langle x| \otimes \tau_{D\bar{D}}^{(x)} \right) - \text{id}_D \otimes \log \left(\sum_x p_x |x\rangle\langle x| \otimes \tau_{\bar{D}}^{(x)} \right) \right. \right. \\
&\quad \left. \left. + \text{id}_{XD\bar{D}} H(D|X\bar{D}) \right)^2 \right] \\
&= V(D|\bar{D}X),
\end{aligned}$$

We are now going to bound the cross term by applying the Cauchy-Schwarz inequality. Using the cyclicity of the trace for $(\rho_{AC}^{(x)})^{1/2}$, we have

$$\begin{aligned}
\text{crossterm} &= \text{tr} \left[\left(\sum_x \sqrt{p_x} |x\rangle\langle x| \otimes (\rho_{AC}^{(x)})^{1/2} \left(\log p_x \rho_{AC}^{(x)} - \text{id}_A \otimes \log \rho_C + \text{id} H(AX|C) \right) \otimes (\tau_{D\bar{D}}^{(x)})^{1/2} \right) \right. \\
&\quad \left. \cdot \left(\sum_x \sqrt{p_x} |x\rangle\langle x| \otimes (\rho_{AC}^{(x)})^{1/2} \otimes (\tau_{D\bar{D}}^{(x)})^{1/2} \left(\log \tau_{D\bar{D}}^{(x)} + \text{id}_{D\bar{D}} \log d_{\bar{D}} + \text{id} H(D|X\bar{D}) \right) \right) \right] \\
&\leq \sqrt{\text{tr}(YY^\dagger) \text{tr}(ZZ^\dagger)},
\end{aligned}$$

where $Y = \sum_x \sqrt{p_x} |x\rangle\langle x| \otimes (\rho_{AC}^{(x)})^{1/2} \left(\log p_x \rho_{AC}^{(x)} - \text{id}_A \otimes \log \rho_C + \text{id} H(AX|C) \right) \otimes (\tau_{D\bar{D}}^{(x)})^{1/2}$ and $Z = \sum_x \sqrt{p_x} |x\rangle\langle x| \otimes (\rho_{AC}^{(x)})^{1/2} \otimes (\tau_{D\bar{D}}^{(x)})^{1/2} \left(\log \tau_{D\bar{D}}^{(x)} + \text{id}_{D\bar{D}} \log d_{\bar{D}} + \text{id} H(D|X\bar{D}) \right)$. We conclude by observing that $\text{tr}(YY^\dagger) = V(AX|C)$ and $\text{tr}(ZZ^\dagger) = V(D|X\bar{D})$. \square

Lemma 3.9. *For a any state ρ_{ABC} , we have*

$$\begin{aligned}
V(AC|B)_\rho &= V(A|B)_\rho + V(C|BA)_\rho \\
&\quad + \text{tr}(\rho_{ABC}(\log \rho_{AB} - \log \rho_B + H(A|B))(\log \rho_{ABC} - \log \rho_{AB} + H(C|BA))) \\
&\quad + \text{tr}(\rho_{ABC}(\log \rho_{ABC} - \log \rho_{AB} + H(C|BA))(\log \rho_{AB} - \log \rho_B + H(A|B))).
\end{aligned} \tag{5}$$

Proof. Direct calculation \square

Lemma 3.10. *Let ρ_{XAB} be of the form $\rho_{XAB} = \sum_{x \in \mathcal{X}} |x\rangle\langle x|_X \otimes \rho_{AB,x}$ with $\text{tr}(\rho_{AB,x} \rho_{AB,x'}) = 0$ when $x \neq x'$. Then we have*

$$V(AX|B)_\rho = V(A|B)_\rho. \tag{6}$$

Proof. Using Lemma 3.9, it suffices to show only the first term of (5) remains. In fact, we have $H(X|BA) = 0$ and

$$\begin{aligned}
V(X|BA)_\rho &= \text{tr}(\rho_{XAB}(\log \rho_{XAB} - \log \rho_{AB})^2) \\
&= \sum_x \text{tr} \left(|x\rangle\langle x|_X \otimes \rho_{AB,x} \left(\sum_{x'} |x'\rangle\langle x'|_X \otimes \log \rho_{AB,x'} - \text{id}_X \otimes \sum_{x'} \log \rho_{AB,x'} \right)^2 \right) \\
&= \sum_x \text{tr} \left(|x\rangle\langle x|_X \otimes \rho_{AB,x} \left(\sum_{x'} (|x'\rangle\langle x'|_X - \text{id}_X)^2 \otimes \log^2 \rho_{AB,x'} \right) \right) \\
&= \sum_x \text{tr} (|x\rangle\langle x|_X (|x\rangle\langle x|_X - \text{id}_X)^2 \otimes \rho_{AB,x} \log^2 \rho_{AB,x}) \\
&= 0 .
\end{aligned}$$

In addition, the other terms are also zero:

$$\begin{aligned}
&\text{tr}(\rho_{XAB}(\log \rho_{AB} - \log \rho_B + H(A|B))(\log \rho_{XAB} - \log \rho_{AB})) \\
&= \sum_x \text{tr} \left((|x\rangle\langle x| \otimes \rho_{AB,x})(\text{id}_X \otimes (\log \rho_{AB} - \log \rho_B + \text{id}_{AB}H(A|B)))(|x\rangle\langle x| \otimes \log \rho_{AB,x} \right. \\
&\quad \left. - \text{id}_X \otimes \sum_{x'} \log \rho_{AB,x'}) \right) \\
&= \sum_x \text{tr} \left(\rho_{AB,x}(\log \rho_{AB} - \log \rho_B + \text{id}_{AB}H(A|B)) \left(\sum_{x' \neq x} \log \rho_{AB,x'} \right) \right) \\
&= 0 ,
\end{aligned}$$

using the orthogonality of $\rho_{AB,x}$ and $\rho_{AB,x'}$, and

$$\begin{aligned}
&\text{tr}[\rho_{XAB}(\log \rho_{XAB} - \log \rho_{AB})(\log \rho_{AB} - \log \rho_B + H(A|B))] \\
&= \sum_x \text{tr} [(|x\rangle\langle x| \otimes \rho_{AB,x})(|x\rangle\langle x| \otimes \rho_{AB,x} - \text{id}_X \otimes \rho_{AB})(\log \rho_{AB} - \log \rho_B + \text{id}_{XAB}H(A|B))] \\
&= \sum_x \text{tr} [(|x\rangle\langle x| \otimes \rho_{AB,x})(|x\rangle\langle x| \otimes \rho_{AB,x} - \text{id}_X \otimes \rho_{AB,x})(\log \rho_{AB} - \log \rho_B + \text{id}_{XAB}H(A|B))] \\
&= 0,
\end{aligned}$$

where we have used the fact that $\rho_{AB,x}\rho_{AB} = \rho_{AB,x}^2$ by the orthogonality conditions. \square

4 Continuity bounds for Rényi divergences

A critical step in the proof is an explicit continuity bound for D_α when α approaches 1. One such bound is given [26, Section 4.2.2]. However, this bound does not give explicit values for the remainder term. The following lemma computes an explicit remainder term for the case of classical probability distributions.

As in [26, Section 4.4.2], we will then apply this lemma to Nussbaum-Szkoła distributions to get a similar result for the Petz divergence D'_α between quantum states.

Lemma 4.1. *Let ρ be a density operator and σ be a not necessarily normalized positive semidefinite operator. Let $\alpha > 1$ and $\mu \in (0, 1)$. Then, we have that*

$$D'_\alpha(\rho\|\sigma) \leq D(\rho\|\sigma) + \frac{(\alpha-1)\ln 2}{2} V(\rho\|\sigma) + (\alpha-1)^2 K_{\rho,\sigma},$$

where

$$K_{\rho,\sigma} = \frac{1}{6\mu^3 \ln 2} 2^{(\alpha-1)(D'_\alpha(\rho\|\sigma)-D(\rho\|\sigma))} \ln^3 \left(2^{(\alpha+\mu-1)(D'_{\alpha+\mu}(\rho\|\sigma)-D(\rho\|\sigma))} + e^2 \right).$$

Proof. As mentioned above, we start by proving the statement for classical probability distributions. Let P be a probability distribution and Q be a not necessarily normalized distribution. Define the random variable X with distribution P , and let $Z = 2^{-D(P\|Q)} \frac{P(X)}{Q(X)}$. Note that for any $\gamma > 0$, we have

$$\mathbb{E}[Z^\gamma] = 2^{-\gamma D(P\|Q)} \sum_x P(x)^{1+\gamma} Q(x)^{-\gamma} \quad (7)$$

$$= 2^{-\gamma(D(P\|Q)-D_{1+\gamma}(P\|Q))}. \quad (8)$$

Now, letting $\nu = \alpha - 1$, we have

$$D_\alpha(P\|Q) = \frac{1}{\nu \ln 2} \ln(\mathbb{E}[Z^\nu]) + D(P\|Q). \quad (9)$$

Applying Taylor's inequality to the function $\nu \mapsto \mathbb{E}[Z^\nu]$ we have

$$\mathbb{E}[Z^\nu] \leq 1 + \nu \mathbb{E}[\ln Z] + \frac{\nu^2}{2} \mathbb{E}[\ln^2 Z] + \frac{\nu^3}{6} \sup_{0 < \gamma \leq \nu} \mathbb{E}[Z^\gamma \ln^3 Z]. \quad (10)$$

Using the fact that $\mathbb{E}[\ln Z] = 0$ and

$$\mathbb{E}[\ln^2 Z] = \sum_x P(x) \left(\ln \frac{P(x)}{Q(x)} - D(P\|Q) \ln 2 \right)^2 \quad (11)$$

$$= (\ln 2)^2 V(P\|Q), \quad (12)$$

together with the inequality $\ln(1+x) \leq x$, we get

$$D_\alpha(P\|Q) \leq D(P\|Q) + \frac{\nu \ln 2}{2} V(P\|Q) + \frac{\nu^2}{6 \ln 2} \sup_{0 < \gamma \leq \nu} \mathbb{E}[Z^\gamma \ln^3 Z]. \quad (13)$$

We now need to bound the remainder term. We want to use the concavity of \ln^3 , but it is only concave on $[e^2, \infty)$. Hence, we start by using the fact that \ln^3 is nondecreasing and $Z^\gamma \geq 0$ to get

$$\mathbb{E}[Z^\gamma \ln^3 Z] = \frac{1}{\mu^3} \mathbb{E}[Z^\gamma \ln^3(Z^\mu)] \quad (14)$$

$$\leq \frac{1}{\mu^3} \mathbb{E}[Z^\gamma \ln^3(Z^\mu + e^2)] \quad (15)$$

$$= \frac{1}{\mu^3} \mathbb{E}[Z^\gamma] \frac{\mathbb{E}[Z^\gamma \ln^3(Z^\mu + e^2)]}{\mathbb{E}[Z^\gamma]}, \quad (16)$$

for any $\mu \in (0, 1]$. Then we use the concavity of the function $t \mapsto \ln^3(t + e^2)$ on $[0, \infty)$ and get

$$\mathbb{E}[Z^\gamma \ln^3 Z] \leq \frac{1}{\mu^3} \mathbb{E}[Z^\gamma] \ln^3 \left(\frac{\mathbb{E}[Z^\gamma(Z^\mu + e^2)]}{\mathbb{E}[Z^\gamma]} \right) \quad (17)$$

$$= \frac{1}{\mu^3} \mathbb{E}[Z^\gamma] \ln^3 \left(\frac{\mathbb{E}[Z^{\mu+\gamma}]}{\mathbb{E}[Z^\gamma]} + e^2 \right) \quad (18)$$

$$= \frac{1}{\mu^3} 2^{\gamma(D_{1+\gamma}(P\|Q) - D(P\|Q))} \ln^3 \left(\frac{2^{(\mu+\gamma)(D_{1+\mu+\gamma}(P\|Q) - D(P\|Q))}}{2^{\gamma(D_{1+\gamma}(P\|Q) - D(P\|Q))}} + e^2 \right) \quad (19)$$

$$\leq \frac{1}{\mu^3} 2^{\gamma(D_{1+\gamma}(P\|Q) - D(P\|Q))} \ln^3 \left(2^{(\mu+\gamma)(D_{1+\mu+\gamma}(P\|Q) - D(P\|Q))} + e^2 \right), \quad (20)$$

where we used the fact that $D_{1+\gamma}(P\|Q) - D(P\|Q) \geq 0$. As this last expression is nondecreasing in γ , we get that

$$\sup_{0 < \gamma \leq \nu} \mathbb{E}[Z^\gamma \ln^3 Z] \leq \frac{1}{\mu^3} 2^{\nu(D_{1+\nu}(P\|Q) - D(P\|Q))} \ln^3 \left(2^{(\mu+\nu)(D_{1+\mu+\nu}(P\|Q) - D(P\|Q))} + e^2 \right). \quad (21)$$

This proves that

$$D_\alpha(P\|Q) \leq D(P\|Q) + \frac{(\alpha - 1) \ln 2}{2} V(P\|Q) + (\alpha - 1)^2 K_{P,Q} \quad (22)$$

with $K_{P,Q} = \frac{1}{6\mu^3 \ln 2} 2^{(\alpha-1)(D_\alpha(P\|Q) - D(P\|Q))} \ln^3 \left(2^{(\alpha+\mu-1)(D_{\alpha+\mu}(P\|Q) - D(P\|Q))} + e^2 \right)$.

Now in order to get the general statement, we use the fact that the Petz divergence between states ρ and σ is equal to the α -divergence of Nussbaum-Szkoła distributions [17], i.e., for all $\alpha \geq 0$

$$D'_\alpha(\rho\|\sigma) = D_\alpha(P^{[\rho,\sigma]}\|Q^{[\rho,\sigma]}) ,$$

for some distributions $P^{[\rho,\sigma]}$ and $Q^{[\rho,\sigma]}$ that only depend on ρ and σ and not on α , and $P^{[\rho,\sigma]}$ and $Q^{[\rho,\sigma]}$ have the same normalization as ρ and σ , respectively. Note that by taking the limit $\alpha \rightarrow 1$, we also get $D(\rho\|\sigma) = D(P^{[\rho,\sigma]}\|Q^{[\rho,\sigma]})$. In addition, by taking the derivative at $\alpha = 1$, we get that $V(\rho\|\sigma) = V(P\|Q)$ [26, Proposition 4.9]. Applying inequality (22) to $P^{[\rho,\sigma]}$ and $Q^{[\rho,\sigma]}$, we get the desired result. \square

Applying Lemma 4.1 to $\rho = \rho_{AB}$, $\sigma = \text{id}_A \otimes \rho_B$ and $\mu = 2 - \alpha$ together with the fact that $D_\alpha(\rho\|\sigma) \leq D'_\alpha(\rho\|\sigma)$, we get

Corollary 4.2. *Let ρ_{AB} be a density operator. Then we have for any $\alpha \in (1, 2)$,*

$$H_\alpha(A|B)_\rho \geq H(A|B)_\rho - \frac{(\alpha - 1) \ln 2}{2} V(A|B)_\rho - (\alpha - 1)^2 K ,$$

where $K = \frac{1}{6(2-\alpha)^3 \ln 2} \cdot 2^{(\alpha-1)(-H'_\alpha(A|B)_\rho + H(A|B)_\rho)} \ln^3 \left(2^{-H'_2(A|B)_\rho + H(A|B)_\rho} + e^2 \right)$.

5 Entropy accumulation with improved second order

We start by recalling the framework for the entropy accumulation theorem [11]. For $i \in \{1, \dots, n\}$, let \mathcal{M}_i be a TPCP map from R_{i-1} to $X_i A_i B_i R_i$, where A_i is finite-dimensional and where X_i represents a classical value from an alphabet \mathcal{X} that is determined by A_i and B_i together. More precisely, we require that, $\mathcal{M}_i = \mathcal{T}_i \circ \mathcal{M}'_i$ where \mathcal{M}'_i is an arbitrary TPCP map from R_{i-1} to $A_i B_i R_i$ and \mathcal{T}_i is a TPCP map from $A_i B_i$ to $X_i A_i B_i$ of the form

$$\mathcal{T}_i(W_{A_i B_i}) = \sum_{y \in \mathcal{Y}, z \in \mathcal{Z}} (\Pi_{A_i, y} \otimes \Pi_{B_i, z}) W_{A_i B_i} (\Pi_{A_i, y} \otimes \Pi_{B_i, z}) \otimes |t(y, z)\rangle \langle t(y, z)|_{X_i}, \quad (23)$$

where $\{\Pi_{A_i, y}\}$ and $\{\Pi_{B_i, z}\}$ are families of mutually orthogonal projectors on A_i and B_i , and where $t : \mathcal{Y} \times \mathcal{Z} \rightarrow \mathcal{X}$ is a deterministic function.

The entropy accumulation theorem stated below will hold for states of the form

$$\rho_{A_1^n B_1^n X_1^n E} = (\mathcal{M}_n \circ \dots \circ \mathcal{M}_1 \otimes \mathcal{I}_E)(\rho_{R_0 E}^0) \quad (24)$$

where $\rho_{R_0 E}^0 \in \mathcal{D}(R_0 \otimes E)$ is a density operator on R_0 and an arbitrary system E . In addition, we require that the Markov conditions

$$A_1^{i-1} \leftrightarrow B_1^{i-1} E \leftrightarrow B_i \quad (25)$$

be satisfied for all $i \in \{1, \dots, n\}$; i.e. $I(A_1^{i-1}; B_i | B_1^{i-1} E)_\rho = 0$.

Let \mathbb{P} be the set of probability distributions on the alphabet \mathcal{X} of X_i , and let R be a system isomorphic to R_{i-1} . For any $q \in \mathbb{P}$ we define the set of states

$$\Sigma_i(q) = \left\{ \nu_{X_i A_i B_i R_i R} = (\mathcal{M}_i \otimes \mathcal{I}_R)(\omega_{R_{i-1} R}) : \omega \in \mathcal{D}(R_{i-1} \otimes R) \text{ and } \nu_{X_i} = q \right\}, \quad (26)$$

where ν_{X_i} denotes the probability distribution over \mathcal{X} with the probabilities given by $\langle x | \nu_{X_i} | x \rangle$. In other words, $\Sigma_i(q)$ is the set of distributions on \mathcal{X} that can be produced at the output of the channel \mathcal{M}_i .

Definition 5.1. A real function f on \mathbb{P} is called a *min-tradeoff function* (or simply tradeoff function for short) for \mathcal{M}_i if it satisfies

$$f(q) \leq \min_{\nu \in \Sigma_i(q)} H(A_i | B_i R)_\nu.$$

Note that if $\Sigma_i(q) = \emptyset$, then $f(q)$ can be chosen arbitrarily. Our result will depend on some simple properties of the tradeoff function, namely the maximum and minimum of f , the minimum of f over valid distributions, and the maximum

variance of f :

$$\begin{aligned}\text{Max}(f) &:= \max_{q \in \mathbb{P}} f(q) \\ \text{Min}(f) &:= \min_{q \in \mathbb{P}} f(q) \\ \text{Min}_\Sigma(f) &:= \min_{q: \Sigma_i(q) \neq \emptyset} f(q) \\ \text{Var}(f) &:= \max_{q: \Sigma_i(q) \neq \emptyset} \sum_{x \in \mathcal{X}} q(x) f(\delta_x)^2 - \left(\sum_{x \in \mathcal{X}} q(x) f(\delta_x) \right)^2.\end{aligned}$$

We write $\text{freq}(X_1^n)$ for the distribution on \mathcal{X} defined by $\text{freq}(X_1^n)(x) = \frac{|\{i \in \{1, \dots, n\} : X_i = x\}|}{n}$. We also recall that in this context, an event Ω is defined by a subset of \mathcal{X}^n and we write $\rho[\Omega] = \sum_{x_1^n \in \Omega} \text{tr}(\rho_{A_1^n B_1^n E, x_1^n})$ for the probability of the event Ω and

$$\rho_{X_1^n A_1^n B_1^n E | \Omega} = \frac{1}{\rho[\Omega]} \sum_{x_1^n \in \Omega} |x_1^n\rangle \langle x_1^n| \otimes \rho_{A_1^n B_1^n E, x_1^n}$$

for the state conditioned on Ω .

Theorem 5.2. *Let $\mathcal{M}_1, \dots, \mathcal{M}_n$ and $\rho_{A_1^n B_1^n X_1^n E}$ be such that (24) and the Markov conditions (25) hold, let $h \in \mathbb{R}$, let f be an affine min-tradeoff function for $\mathcal{M}_1, \dots, \mathcal{M}_n$, and let $\varepsilon \in (0, 1)$. Then, for any event $\Omega \subseteq \mathcal{X}^n$ that implies $f(\text{freq}(X_1^n)) \geq h$,*

$$H_{\min}^\varepsilon(A_1^n | B_1^n E)_{\rho|_\Omega} > nh - c\sqrt{n} - c' \quad (27)$$

holds for

$$\begin{aligned}c &= \sqrt{2 \ln 2} \left(\log(2d_A^2 + 1) + \sqrt{2 + \text{Var}(f)} \right) \sqrt{1 - 2 \log(\varepsilon \rho[\Omega])} \\ c' &= \frac{35(1 - 2 \log(\varepsilon \rho[\Omega]))}{\left(\log(2d_A^2 + 1) + \sqrt{2 + \text{Var}(f)} \right)^2} 2^{2 \log d_A + \text{Max}(f) - \text{Min}_\Sigma(f)} \ln^3 \left(2^{2 \log d_A + \text{Max}(f) - \text{Min}_\Sigma(f)} + e^2 \right)\end{aligned}$$

where d_A is the maximum dimension of the systems A_i .

While the above give reasonable bounds in the general case, in order to obtain better finite n bounds in a particular case of interest, we advise the user to instead use the following bound for an $\alpha \in (1, 2)$ that is either chosen carefully for the problem at hand or computed numerically:

$$H_{\min}^\varepsilon(A_1^n | B_1^n E)_{\rho|_\Omega} \geq nh - n \frac{(\alpha - 1) \ln 2}{2} V^2 - \frac{1}{\alpha - 1} \log \frac{2}{\varepsilon^2 \rho[\Omega]^2} - n(\alpha - 1)^2 K_\alpha, \quad (28)$$

with

$$V = \sqrt{\text{Var}(f) + 2} + \log(2d_A^2 + 1) \quad (29)$$

$$K_\alpha = \frac{1}{6(2 - \alpha)^3 \ln 2} \cdot 2^{(\alpha - 1)(2 \log d_A + (\text{Max}(f) - \text{Min}_\Sigma(f)))} \ln^3 \left(2^{2 \log d_A + (\text{Max}(f) - \text{Min}_\Sigma(f))} + e^2 \right). \quad (30)$$

Note that in general the optimal choice of α will depend on n ; in Theorem 5.2 we have chosen α so that $\alpha - 1$ scales as $\Theta(1/\sqrt{n})$, but other choices are possible. In the case where the systems A_i are classical, we can replace $2 \log d_A$ by $\log d_A$ in (30). This bound holds under the exact same conditions as Theorem 5.2 and for any $\alpha \in (1, 2)$, and this is the bound we use to obtain the numerical results presented in the application presented in Section 6. The choice of α made to get Theorem 5.2 is not the optimal one, but it was chosen to have a relatively simple expression showing the dependence on the main parameters without optimizing the constants.

The proof structure is the same as in [11]. The only difference is when using the continuity of D_α , we use the more precise estimate in Lemma 4.1, and we use the various properties of the entropy variance proven in Section 3 to bound the second-order term.

Proposition 5.3. *Let $\mathcal{M}_1, \dots, \mathcal{M}_n$ and $\rho_{A_1^n B_1^n E}$ be such that (24) and the Markov conditions (25) hold, let $h \in \mathbb{R}$, and let f be an affine min-tradeoff function f for $\mathcal{M}, \dots, \mathcal{M}_n$. Then, for any event Ω which implies $f(\text{freq}(X_1^n)) \geq h$,*

$$H_\alpha^\uparrow(A_1^n | B_1^n E)_{\rho|_\Omega} > nh - n \frac{(\alpha - 1) \ln 2}{2} V^2 - \frac{\alpha}{\alpha - 1} \log \frac{1}{\rho[\Omega]} - n(\alpha - 1)^2 K_\alpha \quad (31)$$

holds for α satisfying $\alpha \in (1, 2)$, and $V = \sqrt{\text{Var}(f) + 2 + \log(2d_A^2 + 1)}$, where d_A is the maximum dimension of the systems A_i and K_α is defined in (30).

Proof. The first step of the proof is to construct a state that will allow us to lower-bound $H_\alpha^\uparrow(A_1^n | B_1^n E)_{\rho|_\Omega}$ using a chain rule similar to the one in Corollary 2.8, while ensuring that the tradeoff function is taken into account. For every i , let $\mathcal{D}_i : X_i \rightarrow X_i D_i$, be a TPCP map defined as

$$\mathcal{D}_i(W_{X_i}) = \sum_{x \in \mathcal{X}} \langle x | W_{X_i} | x \rangle \cdot |x\rangle \langle x|_{X_i} \otimes \tau(x)_{D_i} ,$$

where $\tau(x)$ is such that $H(D_i)_{\tau(x)} = \text{Max}(f) - f(\delta_x)$ (here δ_x stands for the distribution with all the weight on element x). This is possible because $\text{Max}(f) - f(\delta_x) \in [0, \text{Max}(f) - \text{Min}(f)]$ and we choose the dimension of the systems D_i to be equal to $d_D = \lceil 2^{\text{Max}(f) - \text{Min}(f)} \rceil$. More precisely, we fix $\tau(x)$ to be a mixture between a uniform distribution on $\{1, \dots, \lfloor 2^{\text{Max}(f) - f(\delta_x)} \rfloor\}$ and a uniform distribution on $\{1, \dots, \lceil 2^{\text{Max}(f) - f(\delta_x)} \rceil\}$.

Now, let

$$\bar{\rho} := (\mathcal{D}_n \circ \dots \circ \mathcal{D}_1)(\rho) .$$

As in [11], the system D can be thought of as an entropy price that encodes the tradeoff function and it is taken into account by the following fact which is exactly analogous to the corresponding claim in [11]:

$$H_\alpha^\uparrow(A_1^n | B_1^n E)_{\rho|_\Omega} \geq H_\alpha^\uparrow(A_1^n D_1^n | B_1^n E)_{\bar{\rho}|_\Omega} - n \text{Max}(f) + nh . \quad (32)$$

The next step is to relate the entropies on the conditional state $\rho_{|\Omega}$ to those on the unconditional state. To do this, we use Lemma A.1 applied to $\bar{\rho} = \rho[\Omega]\bar{\rho}_{|\Omega} + (\bar{\rho} - \rho[\Omega]\bar{\rho}_{|\Omega})$, together with the fact that $H_\alpha^\dagger \geq H_\alpha$, and obtain

$$H_\alpha^\dagger(A_1^n|B_1^n E)_{\rho_{|\Omega}} \geq H_\alpha(A_1^n D_1^n|B_1^n E)_{\bar{\rho}} - \frac{\alpha}{\alpha-1} \log \frac{1}{\rho[\Omega]} - n\text{Max}(f) + nh. \quad (33)$$

To show the desired inequality (31), it now suffices to prove that $H_\alpha(A_1^n D_1^n|B_1^n E)_{\bar{\rho}}$ is lower bounded by (roughly) $n\text{Max}(f)$.

In order to lower bound $H_\alpha(A_1^n D_1^n|B_1^n E)_{\bar{\rho}}$, we are now going to use the chain rule for Rényi entropies in Corollary 2.8 n times on the state $\bar{\rho}$, with the following substitutions at step i :

- $A_1 \rightarrow A_1^{i-1} D_1^{i-1}$
- $B_1 \rightarrow B_1^{i-1} E$
- $A_2 \rightarrow A_i D_i$
- $B_2 \rightarrow B_i.$

As a result,

$$\begin{aligned} & H_\alpha(A_1^n D_1^n|B_1^n E)_{\bar{\rho}} \\ & \geq \sum_i \inf_{\omega_{R_{i-1}R}} H_\alpha(A_i D_i|B_i R)_{(\mathcal{D}_i \circ \mathcal{M}_i)(\omega)} \\ & \geq \sum_i \left(\inf_{\omega_{R_{i-1}R}} H(A_i D_i|B_i R)_{(\mathcal{D}_i \circ \mathcal{M}_i)(\omega)} - \frac{(\alpha-1)\ln 2}{2} V(A_i D_i|B_i R)_{(\mathcal{D}_i \circ \mathcal{M}_i)(\omega)} - (\alpha-1)^2 K \right), \end{aligned} \quad (34)$$

where we have invoked Corollary 4.2 in the second inequality. Here,

$$K = \frac{1}{6(2-\alpha)^3 \ln 2} \cdot 2^{(\alpha-1)(-\eta_1+\eta_0)} \ln^3 (2^{-\eta_2+\eta_0} + e^2).$$

with $\eta_1 = H'_\alpha(A_i D_i|B_i R)_{(\mathcal{D}_i \circ \mathcal{M}_i)(\omega)}$, $\eta_0 = H(A_i D_i|B_i R)_{(\mathcal{D}_i \circ \mathcal{M}_i)(\omega)}$ and $\eta_2 = H'_2(A_i D_i|B_i R)_{(\mathcal{D}_i \circ \mathcal{M}_i)(\omega)}$.

For any such state $\omega_{R_{i-1}R}$, we have

$$\begin{aligned} H(A_i D_i|B_i R)_{(\mathcal{D}_i \circ \mathcal{M}_i)(\omega)} &= H(A_i X_i D_i|B_i R)_{(\mathcal{D}_i \circ \mathcal{M}_i)(\omega)} \\ &= H(A_i X_i|B_i R)_{\mathcal{M}_i(\omega)} + H(D_i|X_i)_{(\mathcal{D}_i \circ \mathcal{M}_i)(\omega)} \\ &= H(A_i|B_i R)_{\mathcal{M}_i(\omega)} + \sum_x q(x) H(D_i)_{\tau(x)} \\ &= H(A_i|B_i R)_{\mathcal{M}_i(\omega)} + \sum_x q(x) (\text{Max}(f) - f(\delta_x)) \\ &= H(A_i|B_i R)_{\mathcal{M}_i(\omega)} + \text{Max}(f) - f(q), \end{aligned}$$

where $q = \mathcal{M}_i(\omega)_{X_i}$ denotes the distribution of X_i on \mathcal{X} obtained from the state $\mathcal{M}_i(\omega)$. The third equality comes from the fact that X_i is determined by $A_i B_i$.

The last equality holds because f is affine. Using the fact that f is a min-tradeoff function, we get that $H(A_i|B_iR)_{\mathcal{M}_i(\omega)} \geq f(q)$ and therefore:

$$\text{Max}(f) \leq H(A_iD_i|B_iR)_{(\mathcal{D}_i \circ \mathcal{M}_i)(\omega)} \leq \log d_{A_i} + \text{Max}(f) - f(q) .$$

The lower bound allows us to lower bound the first term in Eq. (34). The upper bound will allow us to bound the last term in Eq. (34). In fact, as the systems D_i are classical, we have $\eta_1, \eta_2 \geq -\log d_{A_i}$ by Lemma A.2 (and in the case where A_i are classical, we have $\eta_1, \eta_2 \geq 0$) and thus

$$\begin{aligned} K &\leq \frac{1}{6(2-\alpha)^3 \ln 2} \cdot 2^{(\alpha-1)(\log d_A + \log d_A + \text{Max}(f) - f(q))} \ln^3 \left(2^{\log d_A + \log d_A + \text{Max}(f) - f(q)} + e^2 \right) \\ &\leq \frac{1}{6(2-\alpha)^3 \ln 2} \cdot 2^{(\alpha-1)(2 \log d_A + \text{Max}(f) - \text{Min}_\Sigma(f))} \ln^3 \left(2^{2 \log d_A + \text{Max}(f) - \text{Min}_\Sigma(f)} + e^2 \right) , \end{aligned}$$

as by definition $\Sigma_i(q)$ is not empty (it contains $\mathcal{M}_i(\omega)$).

We now analyze the second term of Eq. (34). Using Lemma 3.10 and then Lemma 3.8 we have

$$V(A_iD_i|B_iR_i)_{(\mathcal{D}_i \circ \mathcal{M}_i)(\omega)} = V(A_iX_iD_i|B_iR_i)_{(\mathcal{D}_i \circ \mathcal{M}_i)(\omega)} \quad (35)$$

$$\leq \left(\sqrt{V(A_i|B_iR_i)_{(\mathcal{D}_i \circ \mathcal{M}_i)(\omega)}} + \sqrt{V(D_i|X_i)_{(\mathcal{D}_i \circ \mathcal{M}_i)(\omega)}} \right)^2 , \quad (36)$$

where for the last equality, we used again Lemma 3.10 and Lemma 3.7.

We bound the first term by the dimension of A using Corollary 3.4.

$$V(A_i|B_iR_i)_{(\mathcal{D}_i \circ \mathcal{M}_i)(\omega)} \leq \log^2(2d_A^2 + 1).$$

For the second term, using the notation $q = \mathcal{M}_i(\omega)_{X_i}$, we have using Lemma 3.6

$$V(D_i|X_i)_{(\mathcal{D}_i \circ \mathcal{M}_i)(\omega)} = \sum_{x \in \mathcal{X}} q(x) V(D_i)_{\tau(x)} + \text{Var}(W) ,$$

where W takes the value $H(D_i)_{\tau(x)} = \text{Max}(f) - f(\delta_x)$ with probability $q(x)$. We have

$$\begin{aligned} \text{Var}(W) &= \sum_{x \in \mathcal{X}} q(x) (\text{Max}(f) - f(\delta_x))^2 - \left(\sum_x q(x) (\text{Max}(f) - f(\delta_x)) \right)^2 \\ &\leq \sup_{\omega, q = \mathcal{M}_i(\omega)_{X_i}} \sum_{x \in \mathcal{X}} q(x) f(\delta_x)^2 - \left(\sum_x q(x) f(\delta_x) \right)^2 \\ &\leq \text{Var}(f) . \end{aligned}$$

To bound $V(D_i)_{\tau(x)}$ recall that $\tau(x)$ is a mixture between the uniform distribution on $\{1, \dots, \lfloor 2^{\text{Max}(f) - f(\delta_x)} \rfloor\}$ and the uniform distribution on $\{1, \dots, \lceil 2^{\text{Max}(f) - f(\delta_x)} \rceil\}$. Note that if $2^{\text{Max}(f) - f(\delta_x)}$ is an integer, $\tau(x)$ is uniformly distributed and thus $V(D_i)_{\tau(x)} = 0$. Assuming $2^{\text{Max}(f) - f(\delta_x)}$ is not an integer, let $\lfloor 2^{\text{Max}(f) - f(\delta_x)} \rfloor = k$. Then $\tau(x)$ is a distribution on $\{1, \dots, k+1\}$ and we have for some p and $p' \leq p$,

$\langle j|\tau(x)|j\rangle = p$ for all $j \in \{1, \dots, k\}$ and $\langle k+1|\tau(x)|k+1\rangle = p'$. The normalization condition is $kp + p' = 1$ and thus, $p' = 1 - kp$. We can now observe that the entropy variance $V(D_i)_{\tau(x)}$ is simply $\text{Var}(-\log p + Z) = \text{Var}(Z)$, where Z is a random variable that is equal to 0 with probability $1 - p'$ and to $\log p - \log p'$ with probability p' . This variance can then be computed as

$$\begin{aligned}\text{Var}(Z) &= \mathbb{E}[Z^2] - \mathbb{E}[Z]^2 \\ &= p'(\log p - \log p')^2 - p'^2(\log p - \log p')^2 \\ &= p'(1 - p') \log^2 \left(\frac{p}{p'} \right).\end{aligned}$$

Now, we use the fact that $\log^2 z \leq 2z$ and continue:

$$\text{Var}(Z) \leq 2p'(1 - p') \frac{p}{p'} \leq 2.$$

As a result,

$$V(D_i|X_i)_{(\mathcal{D}_i \circ \mathcal{M}_i)(\omega)} \leq 2 + \text{Var}(f).$$

Putting everything together, Eq. (33) becomes

$$\begin{aligned}H_\alpha^\uparrow(A_1^n|B_1^n E)_{\rho_{|\Omega}} &\geq nh - n \frac{(\alpha - 1) \ln 2}{2} \left(\log(2d_A^2 + 1) + \sqrt{2 + \text{Var}(f)} \right)^2 \\ &\quad - n(\alpha - 1)^2 K_\alpha - \frac{\alpha}{\alpha - 1} \log \frac{1}{\rho[\Omega]}.\end{aligned}$$

□

Theorem 5.2 is then obtained from Proposition 5.3 by choosing α appropriately.

Proof of Theorem 5.2. We start by lower-bounding the smooth min-entropy by a Rényi entropy: for $\alpha \in (1, 2]$ (see e.g., [26, Proposition 6.5]), we have

$$H_{\min}^\varepsilon(A_1^n|B_1^n E)_{\rho_{|\Omega}} \geq H_\alpha^\uparrow(A_1^n|B_1^n E)_{\rho_{|\Omega}} - \frac{\log(2/\varepsilon^2)}{\alpha - 1}. \quad (37)$$

Then Proposition 5.3 yields for $\alpha \in (1, 1 + \frac{1}{2\ln 2})$

$$\begin{aligned}H_{\min}^\varepsilon(A_1^n|B_1^n E)_{\rho_{|\Omega}} &> nh - n \frac{(\alpha - 1) \ln 2}{2} V^2 - \frac{\alpha}{\alpha - 1} \log \frac{1}{\rho[\Omega]} - n(\alpha - 1)^2 K_\alpha - \frac{\log(2/\varepsilon^2)}{\alpha - 1} \\ &\geq nh - n \frac{(\alpha - 1) \ln 2}{2} V^2 - \frac{1}{\alpha - 1} \log \frac{2}{\varepsilon^2 \rho[\Omega]^2} - n(\alpha - 1)^2 K,\end{aligned} \quad (38)$$

where for the first inequality, K_α is as in (30) and in the second inequality, we used the fact that $\alpha \leq 1 + \frac{1}{2\ln 2}$ and defined

$$K = 12 \cdot 2^{(2\log d_A + (\text{Max}(f) - \text{Min}_\Sigma(f)))} \ln^3 \left(2^{2\log d_A + (\text{Max}(f) - \text{Min}_\Sigma(f))} + e^2 \right).$$

To make the terms in $\alpha - 1$ and $\frac{1}{\alpha-1}$ match, we choose

$$\alpha := 1 + \frac{\sqrt{2 \log \frac{2}{\rho[\Omega]^2 \varepsilon^2}}}{\sqrt{n \ln 2} V}. \quad (39)$$

Assuming that $n \geq \frac{8 \ln 2 \log \frac{2}{\varepsilon^2 \rho[\Omega]^2}}{V^2}$ to have $\alpha \leq 1 + \frac{1}{2 \ln 2}$, we obtain

$$H_{\min}^\varepsilon(A_1^n | B_1^n E)_\rho > nh - \sqrt{n} V \sqrt{(2 \ln 2) \log \frac{2}{\rho[\Omega]^2 \varepsilon^2}} - \frac{2 \log \frac{2}{\rho[\Omega]^2 \varepsilon^2}}{V^2 \ln 2} K. \quad (40)$$

Note that if $n < \frac{8 \ln 2 \log \frac{2}{\varepsilon^2 \rho[\Omega]^2}}{V^2}$ then

$$\sqrt{n} V \sqrt{(2 \ln 2) \log \frac{2}{\rho[\Omega]^2 \varepsilon^2}} > \frac{1}{2} n V^2.$$

As we may assume $h \leq \log d_A$ (otherwise the event Ω will have zero probability) and using the definition of V , we have that

$$\begin{aligned} n \left(h - \frac{1}{2} V^2 \right) &\leq n \log d_A - \frac{1}{2} (\sqrt{2} + \log(2d_A^2 + 1))^2 n \\ &\leq -n \log d_A \end{aligned}$$

which implies that (27) is true in a trivial way. \square

5.1 EAT channels with infrequent sampling

This section can be seen as a user guide to apply the entropy accumulation result presented here in the very common setting where the “testing” is only done in a few rounds that are sampled at random. From the entropy accumulation point of view, the reason for testing is to restrict the optimization involved in the tradeoff function to states $\omega_{R_{i-1}R}$ satisfying the output statistics (26), e.g., winning the CHSH game with a certain probability. However, testing can be costly in terms of randomness or rate and for this reason, the probability of testing, denoted γ is often chosen to be small. We start by defining “channels with infrequent sampling”, which formalizes the concept of a protocol in which we test only a few positions:

Definition 5.4 (Channel with infrequent sampling). A channel with testing probability $\gamma \in [0, 1]$ is an EAT channel $\mathcal{M}_{i, R_{i-1} \rightarrow X_i A_i B_i R_i}$ such that $\mathcal{X} = \mathcal{X}' \cup \{\perp\}$ and that can be expressed as

$$\mathcal{M}_{i, R_{i-1} \rightarrow X_i A_i B_i R_i}(\cdot) = \gamma \mathcal{M}_{i, R_{i-1} \rightarrow X_i A_i B_i R_i}^{\text{test}}(\cdot) + (1 - \gamma) \mathcal{M}_{i, R_{i-1} \rightarrow A_i B_i R_i}^{\text{data}}(\cdot) \otimes |\perp\rangle\langle\perp|_{X_i},$$

where $\mathcal{M}_i^{\text{test}}$ never outputs the symbol \perp on X_i .

The following lemma gives a general way of constructing a tradeoff function f for the map \mathcal{M}_i using a sort of “crossover” tradeoff function g for the map \mathcal{M}_i but using the statistics from $\mathcal{M}_i^{\text{test}}$ only. More precisely, the function g is defined by restricting the input of the map \mathcal{M}_i to be ones that are consistent with the output statistics given by the map $\mathcal{M}_i^{\text{test}}$. The lemma also gives general bounds on the relevant properties of f as a function of γ and simple properties of g .

Lemma 5.5. *Let $\mathcal{M}_i = \mathcal{M}_{R_{i-1} \rightarrow X_i A_i B_i R_i}$ be a channel with testing probability γ as defined above. Assume that the affine function $g : \mathbb{P}(\mathcal{X}') \rightarrow \mathbb{R}$ satisfies for any $q \in \mathbb{P}(\mathcal{X}')$*

$$g(q') \leq \min_{\omega \in \mathcal{D}(R_{i-1} \otimes R)} \{H(A_i | B_i R)_{(\mathcal{M}_i \otimes \mathcal{I}_R)(\omega_{R_{i-1} R})} : ((\mathcal{M}_i^{\text{test}} \otimes \mathcal{I}_R)(\omega_{R_{i-1} R}))_{X_i} = q'\}. \quad (41)$$

Then, the affine function $f : \mathbb{P}(\mathcal{X}) \rightarrow \mathbb{R}$ defined by

$$\begin{aligned} f(\delta_x) &= \text{Max}(g) + \frac{1}{\gamma}(g(\delta_x) - \text{Max}(g)) \quad \forall x \in \mathcal{X}' \\ f(\delta_\perp) &= \text{Max}(g) \end{aligned}$$

is a min-tradeoff function for \mathcal{M}_i . Moreover,

$$\begin{aligned} \text{Max}(f) &= \text{Max}(g) \\ \text{Min}(f) &= \left(1 - \frac{1}{\gamma}\right) \text{Max}(g) + \frac{1}{\gamma} \text{Min}(g) \\ \text{Min}_\Sigma(f) &\geq \text{Min}(g) \\ \text{Var}(f) &\leq \frac{1}{\gamma} (\text{Max}(g) - \text{Min}(g))^2. \end{aligned}$$

Proof. The value for $\text{Min}(f)$ and $\text{Max}(f)$ follow directly from the definition.

To prove that f is a tradeoff function for \mathcal{M}_i , we first determine $\Sigma_i(q)$ (see Definition 5.1). If q is not of the form $q(x) = \gamma q'(x)$ when $x \in \mathcal{X}'$ and $q(\perp) = (1 - \gamma)$ for some $q' \in \mathbb{P}(\mathcal{X}')$, then we know that $\Sigma_i(q) = \emptyset$. So it suffices to focus on distributions q that have this form. Then we have

$$\begin{aligned} f(q) &= \sum_{x \in \mathcal{X}'} q(x) \left(\text{Max}(g) + \frac{1}{\gamma} (g(\delta_x) - \text{Max}(g)) \right) + (1 - \gamma) \text{Max}(g) \\ &= \text{Max}(g) + \sum_{x \in \mathcal{X}'} q'(x) (g(\delta_x) - \text{Max}(g)) \\ &= g(q'). \end{aligned}$$

Using the condition (41), we get

$$\begin{aligned} f(q) = g(q') &\leq \min_{\omega \in \mathcal{D}(R_{i-1} \otimes R)} \{H(A_i | B_i R)_{(\mathcal{M}_i \otimes \mathcal{I}_R)(\omega_{R_{i-1} R})} : ((\mathcal{M}_i^{\text{test}} \otimes \mathcal{I}_R)(\omega_{R_{i-1} R}))_{X_i} = q'\} \\ &\leq \min_{\nu \in \Sigma_i(q)} H(A_i | B_i R)_\nu, \end{aligned}$$

where for the last inequality, we used the fact that for a $\nu \in \Sigma_i(q)$, there exists an $\omega_{R_{i-1}R}$ such that $(\mathcal{M}_i \otimes \mathcal{I}_R)(\omega_{R_{i-1}R}) = \nu$ and $((\mathcal{M}_i^{\text{test}} \otimes \mathcal{I}_R)(\omega_{R_{i-1}R}))_{X_i} = q'$. Thus, f is a min-tradeoff function.

Now for $\text{Min}_\Sigma(f)$, we have

$$\begin{aligned} \text{Min}_\Sigma(f) &= \min_{q: \Sigma_i(q) \neq \emptyset} f(q) \\ &\geq \min_{q' \in \mathbb{P}(\mathcal{X}')} g(q') \\ &= \text{Min}(g) . \end{aligned}$$

Finally, for the variance, we have for q such that $\Sigma_i(q) \neq \emptyset$,

$$\begin{aligned} &\sum_{x \in \mathcal{X}} q(x) \left(f(\delta_x) - \sum_{x \in \mathcal{X}} q(x) f(\delta_x) \right)^2 \\ &= \sum_{x \in \mathcal{X}'} \gamma q'(x) \left(\text{Max}(g) + \frac{1}{\gamma}(g(\delta_x) - \text{Max}(g)) - g(q') \right)^2 + (1 - \gamma)(\text{Max}(g) - g(q'))^2 \\ &= \frac{1}{\gamma} \sum_{x \in \mathcal{X}'} q'(x) \left((\text{Max}(g) - g(\delta_x)) - \gamma(\text{Max}(g) - g(q')) \right)^2 + (1 - \gamma)(\text{Max}(g) - g(q'))^2 . \end{aligned}$$

We can expand the first term and get

$$\begin{aligned} &\frac{1}{\gamma} \sum_{x \in \mathcal{X}'} q'(x) \left((\text{Max}(g) - g(\delta_x)) - \gamma(\text{Max}(g) - g(q')) \right)^2 \\ &= \sum_{x \in \mathcal{X}'} \frac{q'(x)}{\gamma} \left((\text{Max}(g) - g(\delta_x))^2 - 2\gamma(\text{Max}(g) - g(\delta_x))(\text{Max}(g) - g(q')) + \gamma^2(\text{Max}(g) - g(q'))^2 \right) \\ &= \sum_{x \in \mathcal{X}'} \frac{q'(x)}{\gamma} (\text{Max}(g) - g(\delta_x))^2 - 2(\text{Max}(g) - g(q'))^2 + \gamma(\text{Max}(g) - g(q'))^2 \\ &\leq \frac{1}{\gamma} (\text{Max}(g) - \text{Min}(g))^2 - (2 - \gamma)(\text{Max}(g) - g(q'))^2 . \end{aligned}$$

As a result,

$$\text{Var}(f) \leq \frac{1}{\gamma} (\text{Max}(g) - \text{Min}(g))^2 .$$

□

Applying Theorem 5.2 for a map with infrequent sampling, we get a lower bound on the min-entropy of the following form:

$$H_{\min}^\varepsilon \geq nh - c_1 \sqrt{\frac{n}{\gamma}} - c_2 ,$$

where c_1 and c_2 are constants only depend on $\varepsilon, \rho[\Omega], d_A$ and the properties of g but not on n or the testing probability γ . Note that such a bound will be non-trivial as soon as $\gamma \geq \frac{c}{n}$ for some constant c (which corresponds to testing a constant number of rounds). This is to be contrasted with the original entropy accumulation theorem [11] that instead gives a bound of the form $nh - c_1 \frac{\sqrt{n}}{\gamma} - c_2$ and hence will give a trivial bound when $\gamma = o\left(\frac{1}{\sqrt{n}}\right)$.

6 Sample application: Device-independent randomness expansion

We now apply our result to one of the main problems to which the original EAT was applied, namely randomness expansion [5, 6, 19, 31, 15, 2]. This was done using the original EAT in [2], and, to simplify matters, the protocol we will consider here will be essentially the same. The basic task is the following: we are given a pair of devices from a malicious manufacturer; these devices might have been preprogrammed arbitrarily by the manufacturer, but once we have them, they cannot communicate back to the manufacturer. Our goal is to use those devices to generate a uniformly random string, independent from any other data in the universe, and in particular independent from the quantum data the manufacturer might have kept about our devices. It turns out to be impossible to do this without having a little bit of randomness to begin with, but it is possible to expand a small random string into a much longer one.

We give a security proof for the DI-RE protocol based on the CHSH game described in the box below. Recall that the CHSH game works as follows: a referee chooses uniformly random bits X and Y as inputs for the two devices, and the two devices must respond with $A, B \in \{0, 1\}$ respectively without communicating with each other after the questions have been received. The devices win the game if $A \oplus B = XY$ and lose otherwise. The best winning probability for devices using a classical strategy is $3/4$, while the optimal quantum strategy wins with probability $\cos^2(\pi/8) \approx 0.85$. In [2, Equation (12)] (based on [20, Section 2.3]), they give a bound on the amount of randomness produced by the devices assuming that they are using a strategy that allows them to win with probability at least ω ; this bound is given by:

$$H(AB|TE, X = x, Y = y) \geq g^*(\omega) := 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{16\omega(\omega - 1) + 3}\right) \quad (42)$$

for any inputs $x, y \in \{0, 1\}$. This bound is zero at $\omega = 3/4$, one at $\omega = \cos^2(\pi/8)$, and becomes nontrivial as soon as $\omega > 3/4$. The devices are initialized in an arbitrary state by the manufacturer, and at every round of the protocol, we play the game with the devices. To ensure that only a small amount of randomness is consumed by the process of generating the inputs, we randomly choose a small number of test positions (by generating a bit T equal to 1 for test rounds and 0 otherwise), and generate X and Y uniformly at random only for those positions. For the other rounds (that we call the “data” rounds), we always fix the inputs to $X = 0$ and $Y = 0$. In the parameter estimation step of the protocol, the number of test rounds for which $A \oplus B = XY$ is computed. For mathematical convenience, we will choose the positions of the test rounds in an iid manner; i.e. each individual round will have a probability γ of being a test round.

We model the behavior of the devices as follows. We let σ_{ME} be the initial state of the device, M is the system that represents the internal memory of the devices, and E is some reference system that may be in the possession of the manufacturer. Now, let $\mathcal{M}_i : M \rightarrow MT_i X_i Y_i A_i B_i$ be the TPCP map that is applied by the devices in round i . We assume that each of these is of the form

CHSH-based DI-RE protocol

Protocol arguments

- $n \in \mathbb{N}$: number of rounds
- $\gamma \in (0, 1)$: probability that a given position is part of the test set
- $e \in [0, 1]$: minimum fraction of games won that is tolerated
- $r \in \mathbb{R}_+$: generation rate

1. *Distribution:* For $i \in \{1, \dots, n\}$:
 - (a) Generate a random bit T_i such that $\Pr[T_i = 1] = \gamma$.
 - (b) If $T_i = 0$, set $X_i = 0, Y_i = 0$, otherwise, generate X_i and Y_i uniformly over $\{0, 1\}$.
 - (c) Obtain outputs A_i and B_i from the two devices.
2. *Parameter estimation:* Count the number of indices l in the test set for which $A_i \text{ XOR } B_i \neq X_i Y_i$. If $l > (1 - e)\gamma n$, then the protocol is aborted.
3. *Randomness extraction:* Apply some fixed randomness extractor $F : \{0, 1\}^k \times \mathcal{A}^n \times \mathcal{B}^n \rightarrow \{0, 1\}^{rn}$ to a uniform k -bit seed and the string (A_1^n, B_1^n) ; output the result as the final string.

Figure 3: Description of the CHSH-based DI-RE protocol.

depicted in Figure 4, with the position subscript i added to the appropriate systems. The state at the end of step 2 of the protocol is thus:

$$\rho_{MT_1^n X_1^n Y_1^n A_1^n B_1^n E} = (\mathcal{M}_n \circ \dots \circ \mathcal{M}_1) (\sigma_{ME}) ,$$

and we have computed

$$l := |\{i : T_i = 1, A_i \text{ XOR } B_i \neq X_i Y_i\}| .$$

Furthermore, we define Ω as the event that we do not abort after step 2; or, in other words, it is the event that $l \leq (1 - e)\gamma n$. To apply the entropy accumulation theorem to this setting, we need a min-tradeoff function for the \mathcal{M}_i 's. Since Theorem 5.2 demands an affine tradeoff function, the natural choice is to pick the tangent to $g^*(\omega)$ in (42) at a suitably chosen point. We must also ensure that the tradeoff function is defined appropriately for all possible distributions we might observe.¹

We are now going to use entropy accumulation to prove Theorem 6.1 below, which gives a bound on the randomness generation rate r , i.e., the ratio of uniform

¹For instance, we might observe a winning rate strictly above $\cos^2(\pi/8)$ on the testing rounds: if the true winning probability of the devices is very close to optimal, then statistical fluctuations might push us slightly over the edge.

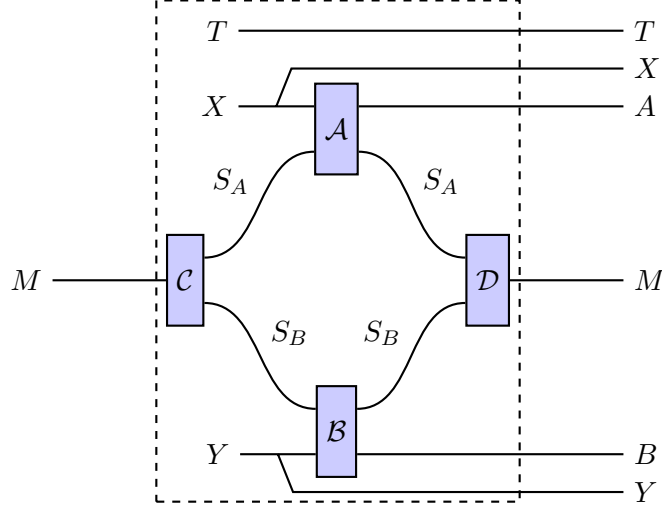


Figure 4: Circuit diagram of $\mathcal{M} : M \rightarrow MTXYAB$. For every round of the protocol, a circuit of this form is applied, where \mathcal{A} and \mathcal{B} are arbitrary TPCP maps with classical output systems A and B , respectively, \mathcal{C} and \mathcal{D} are arbitrary TPCP maps, T is a bit equal to 1 with probability γ , and X and Y are generated uniformly at random whenever $T = 0$, and are fixed to 0, 0 otherwise.

bits that can be generated per round of CHSH. To get a feeling for the sort of entropy production rates that can be expected of this protocol, we have plotted the final rate obtained (i.e. the lower bound on $\frac{1}{n}H_{\min}^{\varepsilon}(A_1^n B_1^n | ET_1^n X_1^n Y_1^n)$) as a function of the block size n when we fix the threshold ε to 0.8, and when we vary the sampling probability γ . The result is in Figure 5. We note that the bounds in the figure are not obtained using the bound stated in Theorem 5.2 directly but rather we used (28) with an α optimized numerically for each point on the curve.

Theorem 6.1. *For any device fulfilling the above conditions and for any $\varepsilon \in (0, 1)$, testing probability $\gamma \in (0, 1)$ and $\frac{3}{4} < e < \cos^2(\frac{\pi}{8})$, after step 2 of the CHSH-based DI-RE protocol, it is the case that either:*

1. *The min-entropy of $\rho_{|\Omega}$ satisfies:*

$$H_{\min}^{\varepsilon}(A_1^n B_1^n | ET_1^n X_1^n Y_1^n)_{\rho_{|\Omega}} > ng^*(e) - \sqrt{\frac{n}{\gamma}}c - c',$$

where $c = \sqrt{2 \ln 2} \left(\log 33 + \sqrt{2 + \frac{1}{\gamma} \left(\frac{dg^*}{d\omega}(e) \right)^2} \right) \sqrt{1 - 4 \log(\varepsilon)}$ and c' is a constant only depending on ε and $\frac{dg^*}{d\omega}(e)$, or

2. *The protocol aborts with probability at least $1 - \varepsilon$.*

First note that applying a Chernoff bound, it is simple to see that provided $e < \cos^2(\pi/8)$, there exist devices that abort the protocol with probability $2^{-\Omega(\gamma n)}$.

In addition, provided one is in the first case, one can obtain a secure random string of length roughly $ng^*(e)$ by choosing the extractor F to be some quantum-proof randomness extractor, such as those presented in [10]. The protocol uses approximately $(h(\gamma) + 2\gamma)n$ random bits, to decide about the testing rounds and to choose the inputs of the players on those rounds and $O(\log^3 n)$ random bits for the seed of the randomness extractor. By taking $\gamma = \Theta(\frac{\log n}{n})$ for instance we have used a polylogarithmic (in n) number of random bits and generated a linear number of bits n , thus achieving exponential randomness expansion. We refer the reader to [7, 15] for further discussions on the way to generate the random bits needed and on the rates of expansion that can be achieved.

Proof. We apply Theorem 5.2 on ρ with the substitutions $A_i \rightarrow A_i B_i$, $B_i \rightarrow T_i X_i Y_i$, and $X_i \rightarrow C_i$, where

$$C_i = \begin{cases} \perp & \text{if } T_i = 0 \\ 1 & \text{if } T_i = 1 \text{ and } A_i \text{ XOR } B_i = X_i Y_i \\ 0 & \text{if } T_i = 1 \text{ and } A_i \text{ XOR } B_i \neq X_i Y_i. \end{cases}$$

Note that X_i is a deterministic function of the classical registers A_i and B_i and the Markov conditions are clearly satisfied.

Note that the maps \mathcal{M}_i correspond to infrequent sampling maps with testing probability γ . As such, to compute a tradeoff function, we use the approach proposed in Lemma 5.5. We start by determining a function $g : \mathbb{P}(\{0, 1\}) \rightarrow \mathbb{R}$ satisfying the property (41). Note that a distribution $q \in \mathbb{P}(\{0, 1\})$ can be uniquely specified by $q(1) \in [0, 1]$. For this reason, we will interpret g as a function $g : [0, 1] \rightarrow \mathbb{R}$. Note that the map $\mathcal{M}_i^{\text{test}}$ is of the form in Figure 4 except that T is fixed to 1 and thus X and Y are chosen uniformly at random, whereas $\mathcal{M}_i^{\text{data}}$ corresponds to T being fixed to 0. The inequality (42) mentioned above shows that g^* satisfies the property (41) required by Lemma 5.5. However, g^* is not an affine function. Nonetheless, g^* is convex so any tangent provides a lower bound. We consider the function obtained by taking the tangent at the point p_b : for $p \in [0, 1]$

$$g_{p_b}(p) = g^*(p_b) + (p - p_b) \frac{dg^*}{d\omega}(p_b). \quad (43)$$

To get the bound stated in the theorem, we simply take $p_b = e$ but depending on γ and n , choosing $p_b < e$ can lead to better bounds. Note that $\text{Max}(g_{p_b}) = g_{p_b}(1)$ and $\text{Min}(g_{p_b}) = g_{p_b}(0)$. Applying Lemma 5.5, we get a min-tradeoff function f defined by $f(\delta_0) = g_{p_b}(1) + \frac{1}{\gamma}(g_{p_b}(0) - g_{p_b}(1))$, $f(\delta_1) = f(\delta_\perp) = g_{p_b}(1)$ and satisfies $\text{Min}_\Sigma(f) \geq g_{p_b}(0)$ and $\text{Var}(f) \leq \frac{1}{\gamma}(g_{p_b}(1) - g_{p_b}(0))^2$.

As previously mentioned Ω is defined to be the event of not aborting, i.e. using the notation of the EAT we have

$$\Omega = \{x_1^n \in \{0, 1, \perp\}^n : |\{i : x_i = 0\}| \leq (1 - e)\gamma n\}.$$

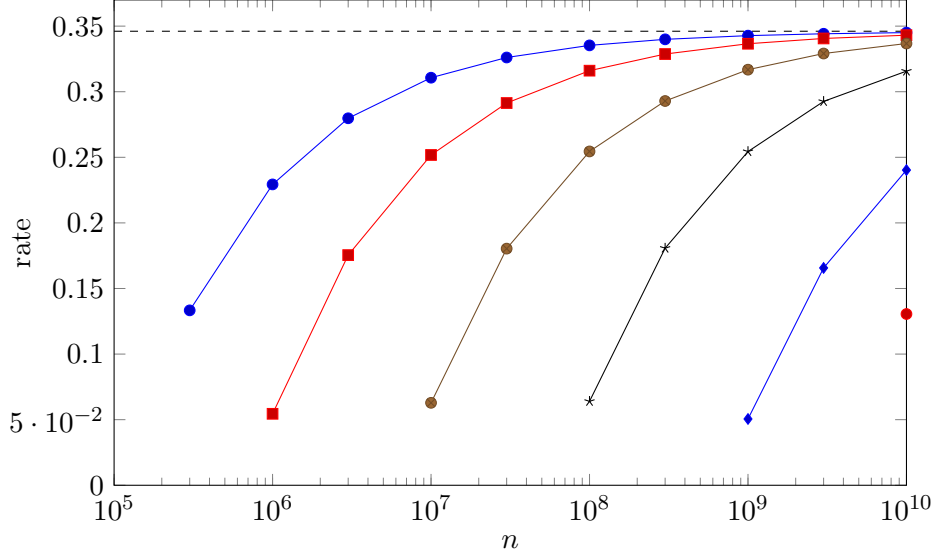


Figure 5: Plot of the final entropy rate achieved as a function of the block size n for several values of the sampling probability γ , when fixing the winning threshold e to 0.8. In decreasing order, we have $\gamma = 1$, $\gamma = 0.1$, $\gamma = 0.01$, $\gamma = 0.001$, $\gamma = 0.0001$, and the last point is $\gamma = 3 \times 10^{-5}$. Here, we fixed $\varepsilon = 10^{-5}$ and assumed that $\rho[\Omega] \geq 10^{-5}$. The dashed line corresponds to the first-order rate of roughly 0.3461, i.e. when $n \rightarrow \infty$.

Observe that we have for $x_1^n \in \Omega$,

$$\begin{aligned}
 f(\text{freq}(x_1^n)) &= \text{freq}(x_1^n)(0)f(\delta_0) + \text{freq}(x_1^n)(1)f(\delta_1) + \text{freq}(x_1^n)(\perp)f(\delta_\perp) \\
 &= \text{freq}(x_1^n)(0) \left(g_{p_b}(1) - \frac{1}{\gamma}(g_{p_b}(1) - g_{p_b}(0)) \right) + (1 - \text{freq}(x_1^n)(0))g_{p_b}(1) \\
 &\geq g_{p_b}(1) + (1 - e)(g_{p_b}(0) - g_{p_b}(1)) \\
 &= g_{p_b}(e) .
 \end{aligned}$$

Note that if $\Pr[\Omega] < \varepsilon$, then we are in case 2 of the theorem, so we will assume that $\rho[\Omega] = \Pr[\Omega] \geq \varepsilon$. Applying Theorem 5.2, we get

$$H_{\min}^\varepsilon(A_1^n B_1^n | ET_1^n X_1^n Y_1^n)_{\rho|\Omega} > n g_{p_b}(e) - \sqrt{\frac{n}{\gamma}} c - c',$$

where $c = \sqrt{2 \ln 2} \left(\log 33 + \sqrt{2 + \frac{1}{\gamma} \left(\frac{dg^*}{d\omega}(p_b) \right)^2} \right) \sqrt{1 - 4 \log(\varepsilon)}$ and c' is a constant only depending on ε and $\frac{dg^*}{d\omega}(p_b)$. \square

7 Conclusion and open problems

The new version of the entropy accumulation theorem presented here can now be applied directly to protocols with infrequent sampling (or to other situations

where the entropy variance is significantly different from the local dimension) without paying too heavy a price. In particular, in the infrequent sampling case, the scaling in the sampling frequency γ roughly matches what we would expect in the classical i.i.d. case from Chernoff-type bounds.

While this is largely good enough in practice, there are still open questions remaining. First: can we find a version of the theorem with an optimal second-order term? Ideally, we could hope for a second-order term that matches what we see in the i.i.d. case, which would look like $\sqrt{nV}\Phi^{-1}(\varepsilon^2)$ (e.g., in [28]), where Φ is the cumulative distribution function of a Gaussian distribution, and V would be an appropriate entropy variance term. Here we fall short of this in two ways: first, our V quantity is the result of applying some inequalities in the proof (see Equation (36)) that are not always tight; this may however be unavoidable if one wants to have a clean expression in terms of $\text{Var}(f)$. The second issue is that the dependence in ε does not match the $\Phi^{-1}(\varepsilon)$ or $\Phi^{-1}(\varepsilon^2)$ that is usually seen in second-order expansions, but is instead similar to what is done in the fully quantum AEP of [25] and in the original EAT. This also seems very difficult to overcome in our situation, since these terms usually arise from an application of the Berry-Esseen theorem, which quantifies how much a sum of iid random variables diverges from a normal distribution, and therefore depends very strongly on the iid assumption which we do not have here.

We could also scale back our goals a bit and try to improve the last term, namely the c' in Equation (27). As it stands, this term arises from a sequence of ad-hoc inequalities that could very well be improved. It would be particularly interesting to understand which parameters this term should “really” depend on: for example, the expression we give here depends on $\rho[\Omega]$ and ε , but this may well be an artifact of our choice of α in the proof. We thus leave these questions as open problems.

A Various lemmas

Lemma A.1 (Lemma B.5 in [11]). *Let ρ_{AB} be a quantum state of the form $\rho = \sum_x p_x \rho_{AB|x}$, where $\{p_x\}$ is a probability distribution over \mathcal{X} . Then, for any $x \in \mathcal{X}$ and any $\alpha \in (1, \infty)$,*

$$H_\alpha^\uparrow(A|B)_\rho - \frac{\alpha}{\alpha-1} \log \left(\frac{1}{p_x} \right) \leq H_\alpha^\uparrow(A|B)_{\rho_{|x}}. \quad (44)$$

and for $\alpha \in (0, 1)$,

$$H_\alpha^\uparrow(A|B)_\rho - \frac{\alpha}{\alpha-1} \log \left(\frac{1}{p_x} \right) \geq H_\alpha^\uparrow(A|B)_{\rho_{|x}}. \quad (45)$$

Lemma A.2. *Let $\rho_{ABX} = \sum_x p_x \rho_{AB}(x) \otimes |x\rangle\langle x|_X$ be a quantum state with X classical. Then, for any $\alpha \in (0, 1) \cup (1, 2]$, we have*

$$H'_\alpha(AX|B) \geq -\log d_A.$$

Proof. First, let us define the extension $\rho_{ABXX'} = \sum_x p_x \rho_{AB}(x) \otimes |xx\rangle\langle xx|_{XX'}$, and observe that by data processing, $H'_\alpha(AX|B) \geq H'_\alpha(AX|BX')$. Thus,

$$\rho_{ABXX'}^\alpha \rho_{BX'}^{1-\alpha} = \sum_x p_x \rho_{AB}(x)^\alpha \rho_B(x)^{1-\alpha} \otimes |xx\rangle\langle xx|_{XX'}$$

and therefore

$$\begin{aligned} H'_\alpha(AX|B) &\geq H'_\alpha(AX|BX') \\ &= \frac{1}{1-\alpha} \log \sum_x p_x 2^{(1-\alpha)H'_\alpha(A|B, X=x)_\rho} \\ &\geq \frac{1}{1-\alpha} \log \sum_x p_x 2^{(\alpha-1) \log d_A} \\ &\geq -\log d_A. \end{aligned}$$

□

Acknowledgments

The authors would like to thank Rotem Arnon-Friedman for bringing to our attention the suboptimal dependence on the testing probability in the original entropy accumulation theorem and Renato Renner for his comments.

References

- [1] Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner, and Thomas Vidick. “Practical device-independent quantum cryptography via entropy accumulation”. In: *Nature Communications* 9.1 (2018), p. 459.
- [2] Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick. *Simple and tight device-independent security proofs*. 2016. arXiv: [1607.01797](#).
- [3] Salman Beigi, Nilanjana Datta, and Felix Leditzky. “Decoding quantum information via the Petz recovery map”. In: *Journal of Mathematical Physics* 57.8 (2016), p. 082203. DOI: [10.1063/1.4961515](#). arXiv: [1504.04449](#).
- [4] Salman Beigi and Amin Gohari. “Quantum achievability proof via collision relative entropy”. In: *IEEE Transactions on Information Theory* 60.12 (Dec. 2014), pp. 7980–7986. DOI: [10.1109/TIT.2014.2361632](#). arXiv: [1312.3822](#).
- [5] Roger Colbeck. “Quantum and relativistic protocols for secure multi-party computation”. PhD thesis. University of Cambridge, 2006. arXiv: [0911.3814](#).
- [6] Roger Colbeck and Adrian Kent. “Private Randomness Expansion With Untrusted Devices”. In: *J. Phys. A - Math. Gen.* 44 (9 2011), p. 095305. arXiv: [1011.4474](#).

- [7] Matthew Coudron, Thomas Vidick, and Henry Yuen. “Robust randomness amplifiers: Upper and lower bounds”. In: *Proc. APPROX-RANDOM*. Springer, 2013, pp. 468–483. arXiv: [1305.6626](#).
- [8] Nilanjana Datta and Felix Leditzky. “Second-order asymptotics for source coding, dense coding, and pure-state entanglement conversions”. In: *IEEE Transactions on Information Theory* 61.1 (Jan. 2015), pp. 582–608. DOI: [10.1109/TIT.2014.2366994](#). arXiv: [1403.2543](#).
- [9] Nilanjana Datta, Yan Pautrat, and Cambyse Rouzé. “Second-order asymptotics for quantum hypothesis testing in settings beyond i.i.d.—quantum lattice systems and more”. In: *Journal of Mathematical Physics* 57.6 (2016), p. 062207. DOI: [10.1063/1.4953582](#). arXiv: [1510.04682](#).
- [10] Anindya De, Christopher Portmann, Thomas Vidick, and Renato Renner. “Trevisan’s extractor in the presence of quantum side information”. In: *SIAM J. Comput.* 41.4 (2012), pp. 915–940. arXiv: [0912.5514](#).
- [11] Frédéric Dupuis, Omar Fawzi, and Renato Renner. *Entropy accumulation*. 2016. arXiv: [1607.01796](#).
- [12] Masahito Hayashi. “Information spectrum approach to second-order coding rate in channel coding”. In: *IEEE Transactions on Information Theory* 55.11 (Nov. 2009), pp. 4947–4966. DOI: [10.1109/TIT.2009.2030478](#). arXiv: [0801.2242 \[cs.IT\]](#).
- [13] Felix Leditzky. “Relative entropies and their use in quantum information theory”. PhD thesis. University of Cambridge, 2016. arXiv: [1611.08802](#).
- [14] Ke Li. “Second-order asymptotics for quantum hypothesis testing”. In: *Annals of Statistics* 42.1 (Feb. 2014), pp. 171–189. DOI: [10.1214/13-AOS1185](#). arXiv: [1208.1400](#).
- [15] Carl A Miller and Yaoyun Shi. *Universal security for randomness expansion*. 2014. arXiv: [1411.6608](#).
- [16] Martin Müller-Lennert, Frédéric Dupuis, Oleg Szehr, Serge Fehr, and Marco Tomamichel. “On quantum Rényi entropies: a new generalization and some properties”. In: *Journal of Mathematical Physics* 54.12, 122203 (2013). DOI: [10.1063/1.4838856](#). arXiv: [1306.3142](#).
- [17] Michael Nussbaum and Arleta Szkola. “The Chernoff lower bound for symmetric quantum hypothesis testing”. In: *Annals of Statistics* 37.2 (2009), pp. 1040–1057. DOI: [10.1214/08-AOS593](#). arXiv: [quant-ph/0607216](#).
- [18] Dénes Petz. “Quasi-entropies for finite quantum systems”. In: *Reports on Mathematical Physics* 23.1 (1986), pp. 57–65. DOI: [10.1016/0034-4877\(86\)90067-4](#).
- [19] S. Pironio, A. Acín, S. Massar, A.B. de La Giroday, D.N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T.A. Manning, et al. “Random numbers certified by Bell’s theorem”. In: *Nature* 464.7291 (2010), pp. 1021–1024. arXiv: [0911.3427](#).

- [20] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. “Device-independent quantum key distribution secure against collective attacks”. In: *New Journal of Physics* 11.4 (2009), p. 045021. DOI: [10.1088/1367-2630/11/4/045021](#). arXiv: [0903.4460](#).
- [21] Yury Polyanskiy. “Channel coding: non-asymptotic fundamental limits”. PhD thesis. Princeton University, 2010.
- [22] Yury Polyanskiy, H. Vincent Poor, and Sergio Verdú. “Channel Coding Rate in the Finite Blocklength Regime”. In: *Information Theory, IEEE Transactions on* 56.5 (May 2010), pp. 2307–2359. DOI: [10.1109/TIT.2010.2043769](#).
- [23] Volker Strassen. “Asymptotische Abschätzungen in Shannons Informationstheorie”. In: *Trans. 3rd Prague Conf. Inf. Theory*. 1962, pp. 689–723.
- [24] M. Tomamichel. “A Framework for Non-Asymptotic Quantum Information Theory”. PhD thesis. ETH Zurich, 2012. arXiv: [1203.2142](#).
- [25] M. Tomamichel, R. Colbeck, and R. Renner. “A fully quantum asymptotic equipartition property”. In: *IEEE Trans. Inform. Theory* 55 (2009), pp. 5840–5847. arXiv: [0811.1221](#).
- [26] Marco Tomamichel. *Quantum Information Processing with Finite Resources: Mathematical Foundations*. Vol. 5. Springer, 2015. arXiv: [1504.00233](#).
- [27] Marco Tomamichel, Roger Colbeck, and Renato Renner. “Duality between smooth min- and max-entropies”. In: *IEEE Trans. Inform. Theory* 56 (2010), p. 4674. arXiv: [0907.5238](#).
- [28] Marco Tomamichel and Masahito Hayashi. “A Hierarchy of Information Quantities for Finite Block Length Analysis of Quantum Tasks”. In: *IEEE Transactions on Information Theory* 59.11 (Nov. 2013), pp. 7693–7710. DOI: [10.1109/TIT.2013.2276628](#). arXiv: [1208.1478](#).
- [29] Marco Tomamichel and Vincent Y. F. Tan. “Second-Order Asymptotics for the Classical Capacity of Image-Additive Quantum Channels”. In: *Communications in Mathematical Physics* 338.1 (2015), pp. 103–137. DOI: [10.1007/s00220-015-2382-0](#).
- [30] Marco Tomamichel and Vincent Y. F. Tan. “Second-Order Coding Rates for Channels With State”. In: *Information Theory, IEEE Transactions on* 60.8 (Aug. 2014), pp. 4427–4448. DOI: [10.1109/TIT.2014.2324555](#).
- [31] Umesh Vazirani and Thomas Vidick. “Certifiable quantum dice: or, true random number generation secure against quantum adversaries”. In: *Proc. ACM STOC*. ACM. 2012, pp. 61–76. arXiv: [1111.6054](#).
- [32] Mark M. Wilde, Andreas Winter, and Dong Yang. “Strong converse for the classical capacity of entanglement-breaking and Hadamard channels via a sandwiched Rényi relative entropy”. In: *Communications in Mathematical Physics* 331.2 (2014), pp. 593–622. DOI: [10.1007/s00220-014-2122-x](#). arXiv: [1306.1586](#).